INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO ACRE

FABRÍCIO SOUZA FERRARI
THIAGO SOUSA BARBOSA GOMES

PROTÓTIPO DE SISTEMA DE RECONHECIMENTO FACIAL COM USO DE DRONE PARA SEGURANÇA PÚBLICA

Rio Branco
2022

FABRÍCIO SOUZA FERRARI
THIAGO SOUSA BARBOSA GOMES

PROTÓTIPO DE SISTEMA DE RECONHECIMENTO FACIAL COM USO DE DRONE PARA SEGURANÇA PÚBLICA

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Sistemas para Internet do Instituto Federal de Educação, Ciência e Tecnologia do Acre, Campus Rio Branco, em cumprimento às exigências legais como requisito parcial à obtenção do título de Tecnólogo em Sistemas para Internet.

Orientador: Breno Carrillo Silveira, Mestre.

Rio Branco
2022

FABRÍCIO SOUZA FERRARI
THIAGO SOUSA BARBOSA GOMES

PROTÓTIPO DE SISTEMA DE RECONHECIMENTO FACIAL COM USO DE DRONE PARA SEGURANÇA PÚBLICA

Trabalho de Conclusão de Curso apresentado ao Curso Tecnólogo em Sistema para Internet do Instituto Federal de Educação, Ciência e Tecnologia do Acre, Campus Rio Branco, em cumprimento às exigências legais como requisito parcial à obtenção do título de Tecnólogo em Sistemas para Internet.

Trabalho de Conclusão de Curso apresentado e aprovado em 04/04/2022, pela seguinte Banca Examinadora:

Prof. Mestre Breno Carrillo Silveira - Presidente
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Prof. Doutor Darueck Acácio Campos, Secretário da Banca Examinadora
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Prof. Mestre Diego Canizio Lopes, Membro da Banca Examinadora
Instituto Federal de Educação, Ciência e Tecnologia do Acre

Dedicatória

Foi pensando nas pessoas que executei este projeto, por isso dedico este trabalho principalmente a todos aqueles a quem esta pesquisa possa salvar e ajudar de alguma forma no futuro, assim como meu orientador, meus familiares e colegas que me ajudaram na implementação deste trabalho.

Fabrício Souza Ferrari

Dedico este trabalho à minha mãe, que me motivam a evoluir cada vez mais em minha vida profissional e pessoal, não medindo esforços para me proporcionar um ensino de qualidade mesmo diante de todas as dificuldades.

Thiago Sousa Barbosa Gomes

AGRADECIMENTO

O desenvolvimento desse trabalho de conclusão de curso contou com a ajuda de diversas pessoas, dentre as quais agradeço:

Ao professor Breno Carrillo Silveira, por ter sido nosso orientador e ter desempenhado tal função com dedicação, comprometimento e amizade.

Aos demais professores do curso, que apesar de não estarem envolvidos diretamente no trabalho, foram suas correções e ensinamentos que me permitiram apresentar um melhor desempenho no meu processo de formação.

Aos meus familiares, principalmente minha irmã Vanuza de Souza Ferrari, meu pai Ruy Luiz Ferrari e minha mãe Inês Ribeiro de Souza Ferrari por todo o apoio e pela ajuda, que muito contribuíram para a realização deste trabalho.

Fabrício Souza Ferrari

Em primeiro lugar agradeço a Deus por sempre ter me dado força para completar meus desafios ao longo dos anos, agradeço a minha família que sempre me apoiaram nos momentos mais difíceis especialmente minha Mãe pelo apoio, força e amor incondicional. Sem o apoio dela isso jamais teria sido possível. Gostaria de agradecer a todos os meus amigos que sempre me incentivaram nos momentos difíceis e sempre me motivaram a continuar de cabeça erguida nos momentos mais extremos. Por fim, agradeço ao meu Orientador Breno Silveira, por toda dedicação e exemplo profissional e pessoal, que sempre me inspirou a dar meu melhor nessa etapa de tamanha importância.

Thiago Sousa Barbosa Gomes

"Aquele que se empenha a resolver as dificuldades resolve-as antes que elas surjam. Aquele que se ultrapassa a vencer os inimigos triunfa antes que as suas ameaças se concretizem."

Sun Tzu

RESUMO

O Artigo 144 da Constituição Federal do Brasil de 1988 determina que a segurança pública é dever do Estado e é direito e responsabilidade de todos. Nesse diapasão, faz-se necessário um esforço coletivo para que novas tecnologias, processos e métodos sejam implementados, para melhorar a vida das pessoas, tanto por parte do poder público e da sociedade civil. A utilização de recursos tecnológicos, como o emprego de drones tende a melhorar os serviços em segurança pública e, consequentemente proporcionar maior segurança aos cidadãos. Dessa forma, o trabalho apresentou a proposta de implementação de um protótipo de reconhecimento facial, com classificação do agente identificado e com a determinação de sua localização, para auxiliar o operador em segurança pública em suas atividades. Empregando técnicas de Inteligência Artificial e de *Machine Learning* foi possível desenvolver o algoritmo para tal. Ao término do trabalho restou constatado a funcionalidade do protótipo e suas aplicações.

Palavras-chave: Reconhecimento Facial. Drones. Machine Learning. Segurança Pública.

ABSTRACT

Article 144 of the Federal Constitution of Brazil of 1988 determines that public security is a duty of the State and everyone's right and responsibility. In this vein, a collective is necessary so that new technologies, processes and methods are implemented, to improve people's lives, both on the part of public authorities and civil society. The use of technological resources, such as the use of drones, tends to improve public safety services and, consequently, provide greater security to citizens. In this way, the proposed work of implementing a facial recognition mechanism, with identified classification and with the determination of its location, will help the operator in public safety. Using Artificial Intelligence and Machine Learning techniques, it was possible to develop the development for this. At the end of the work, the functionality of the operation and its applications remained.

Keywords: Facial recognition. Drones. Machine Learning. Public Security.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O Artigo 144 da Constituição Federal do Brasil de 1988 determina que a segurança pública é dever do Estado e é direito e responsabilidade de todos. Nesse diapasão, faz-se necessário um esforço coletivo para que novas tecnologias, processos e métodos sejam implementados, para melhorar a vida das pessoas, tanto por parte do poder público e da sociedade civil.

Diante disso, pesquisas científicas e tecnológicas possuem um importante papel na contribuição para o uso eficaz do recurso público empregado na segurança. Inovações em processos, em artefatos e na própria forma de se ver a segurança pública, são elementos essenciais para melhorar ações preventivas e repressivas que possam garantir a integridade física e patrimonial do cidadão de bem.

Ainda, avanços tecnológicos, além de otimizarem o uso dos recursos, especialmente dos operadores em segurança pública, colaboram para proporcionar maior segurança para estes realizarem suas atividades e para que ações policiais possam prevenir ações delituosas ou identificar possíveis agentes, inibindo o ciclo do crime.

Nesse cenário, as tecnologias da informação e da comunicação são essenciais. O emprego de um simples localizador com o cadastro georreferenciado dos logradouros da cidade, facilitará o atendimento de uma ocorrência emergencial. A utilização de aplicativos em dispositivos móveis, que possam realizar pesquisas sobre indivíduos, nas viaturas policiais facilitará ações preventivas na busca de uma sociedade mais segura. O emprego de câmeras facilita a cobertura de áreas sem o emprego direto de um elevado contingente de profissionais.

Considerando que agente público deve servir e proteger a sociedade, salvaguardar a vida de possíveis vítimas e preservar a incolumidade física e patrimonial das pessoas, qualquer ferramenta que otimize seu trabalho, afetará diretamente a vida de cidadãos que só desejam viver com maior segurança.

Além disso, o emprego de novas tecnologias também contribui para a própria preservação da segurança dos operadores em segurança pública. Quando um processo é automatizado e recursos tecnológicos são utilizados entre o agente delituoso e o servidor público responsável por prestar serviços em segurança, o operador fica menos suscetível ao risco inerente aos atos de seu trabalho.

Dessa forma, é importante inovar e criar mecanismos para que o poder público preste um serviço com a maior qualidade possível, usando o erário com parcimônia e proporcionando segurança para os cidadãos.

Nesse contexto, o presente trabalho apresenta um protótipo que pode ser utilizado na segurança pública para atividades preventivas, investigativas e até mesmo repressivas: o uso de reconhecimento facial com o emprego de drones.

Atualmente drones são utilizados para as mais diversas atividades: lazer, gravações de vídeos em espaços aberto, mapeamento e georreferenciamento em propriedades, entre outros. Tais veículos não tripulados evitam o trânsito urbano em vias públicas e conseguem se deslocar com maior facilidade pelo ar.

Assim, é perfeitamente plausível o emprego de drones para atividades em segurança pública, desde o processo de monitoramento de áreas com elevados índices de criminalidade, prevenções de delitos em longos espaços e/ou na identificação de agentes delituosos com registros no sistema judiciário penal brasileiro.

Nesse engendramento, o presente trabalho implementou um protótipo com emprego de drone para o reconhecimento facial de agentes que possam apresentar algum risco para sociedade. Como base em técnicas de IA e *Machine Learning*, foi possível desenvolver um algoritmo que, a partir de imagens transmitidas em tempo real por um drone, reconheçam um cidadão e seu potencial de risco para o ambiente que o cerca.

Cabe observar que o modelo classificatório de risco por parte de um suposto agente foi implementado como proposta para mostrar a efetividade do algoritmo, das técnicas e do uso de um bioma de tecnologias para reconhecimento facial, georreferenciado, de uma pessoa.

A ideia básica é proporcionar ao operador em segurança pública a identificação de um possível agente delituoso, de seu potencial (risco) para a sociedade (de acordo com seus histórico e ficha criminal) e sua localização; tanto em uma ação preventiva, quanto investigativa ou repressiva.

Cabe observar que os critérios de classificação não se esgotam. O modelo pode se expandido ou alterado de acordo com a necessidade de um órgão específico da segurança pública ou de uma atividade policial mais específica. Entretanto, resta constatado no trabalho a efetividade do emprego das ferramentas de desenvolvimento e de artefatos tecnológicos que auxiliem as forças de segurança no combate e prevenção ao crime.

Seguinte os fatos supracitados, a proposta do trabalho se constituiu na implementação de um protótipo de reconhecimento facial utilizando ferramentas de *IA e Machine Learning*, com base em imagens transmitidas em tempo real por um drone.

O trabalho se justifica ao passo que o emprego de tal tecnologia pode colaborar para redução da criminalidade e para uma melhor oferta de serviços em segurança pública para a população, auxiliando o operador na realização de suas atividades.

Nesse cenário, resta constatado a importância do trabalho ao passo que fomenta o desenvolvimento de uma tecnologia que possa otimizar a tarefa policial e o salvaguardo da segurança da população. Ainda, nenhuma política pública em segurança no estado do Acre ousou realizar algo semelhante.

Além da introdução, o trabalho está subdividido em desenvolvimento (abordando conceitos teóricos), implementação do protótipo (citando como o protótipo foi desenvolvido) e conclusões.

2 DESENVOLVIMENTO

Este capítulo é composto pelo referencial teórico, o referencial analítico, e pela apresentação e análise dos resultados.

2.1 REFERENCIAL TEÓRICO

Inicialmente serão abordados conceitos sobre inteligência artificial, *Machine Learning* e redes neurais; encerrando o debate teórico com tópicos de biometria facial e elementos concernentes ao modelo de algoritmo de reconhecimento facial utilizado.

2.1.1 Definições Teóricas Sobre Reconhecimento Facial

2.1.1.1 Inteligência Artificial

A inteligência artificial, mais conhecida como IA, pode ser classificada como um ramo de estudo da ciência da computação que versa especificamente sobre emular, através de uma máquina, aspectos e comportamentos da inteligência humana. Segundo Boose (1994), citado por Fernandes (2005, p. 2):

> A inteligência artificial busca entender a mente humana e imitar seu comportamento, levantando questões como: Como ocorre o pensar? Como o homem extrai o conhecimento no mundo? Como a memória, os sentidos e a linguagem ajudam no desenvolvimento da inteligência? Como surgem as ideias? Como a mente processa informações e tira conclusões decidindo por uma coisa ao invés de outra? Essas são as perguntas que a IA precisa responder para simular o raciocínio humano e implementar aspectos de inteligência.

Obviamente imitar a inteligência humana não é algo fácil. A complexidade da psiquê dificulta sua simulação em algoritmos. Segundo Fernandes (2005, p. 2),

> "o objetivo da IA é o estudo e a modelagem da inteligência tratada como um fenômeno. A inteligência é algo extremamente complexo, resultado de milhões de anos de evolução. Entendê-la não é tarefa fácil. Embora existam muitas conclusões relevantes, ainda há muito a ser desvendado, uma vez que não existe uma teoria completa sobre a mente humana e o processo de raciocínio."

Entretanto, todo o conhecimento já acumulado sobre IA já proporcionaram diversos avanços em várias outras áreas do conhecimento e em aplicações de uso mais convencional.

Usando a Inteligência Artificial já é possível, através de processos seletivos de aprendizado, simular alguns comportamentos humanos como reconhecimento de imagem e cores, reconhecimento de fala e respostas a ações específicas baseadas em comportamentos anteriores.

Mais, através das aplicações dos processos seletivos de aprendizado e do comportamento de uma IA, é possível resolver problemas de maneira automatizada e com margem de erro aceitável.

Para uma maior compreensão dos conceitos fundamentais de IA, é interessante saber sobre o "pai" da Inteligência Artificial.

2.1.1.2 O "Pai" da Inteligência Artificial

Alan Turing (1912-1954) foi um matemático brilhante e hoje muito reconhecido por suas inúmeras contribuições em diversos temas. Foi pioneiro em aspectos como lógica, criptoanálise e é considerado por muitos como o pai da ciência computacional, ciência cognitiva, vida artificial e da Inteligência Artificial.

Em 1936 publicou um artigo que descrevia detalhadamente um modelo de uma máquina algorítmica abstrata, cuja a função era materializar a lógica humana e solucionar qualquer cálculo representado no formato de um algoritmo, que seriam exibidos no formato de instruções a serem processadas de forma mecânica. O artefato ficou conhecido como "A máquina de Turing" (TURING, A. M.; COPELAND, B. J., 2010), que pode ser dita como protótipo ou base essencial na concepção dos computadores de hoje.

Alan Turing também é o responsável por criar uma máquina capaz de decifrar a estratégia de criptografia baseada na máquina Enigma criada pelos alemães durante a Segunda

Guerra Mundial em 1940. O desenvolvimento do artefato proporcionou uma grande vantagem aos aliados durante a guerra.

Especificamente em relação aos conceitos basilares de IA, em uma palestra no início de 1947, intitulada de "*Lecture on the Automatic Computing Engine*" (que pode ser traduzido livremente em algo como "*Palestra sobre uma máquina de computação automática*" ou "*Palestra sobre um motor de computação automática")*, Turing apresentou pela primeira vez ao público seu novo conceito de Inteligência Artificial.

Turing também foi o primeiro a publicar um texto que fazia referência a uma visão mais completa sobre IA em seu artigo de 1950 "*Computing Machinery and Intelligency*". Apresentou o Teste de Turing, onde sugeriu um teste que determinaria se uma máquina era pensante. O computador passaria no teste se um interrogador humano, depois de propor algumas perguntas por escrito, não conseguisse discernir se as respostas foram respondidas por uma pessoa ou não.

Com base nessa rápida visão sobre o surgimento dos conceitos de IA, é possível versar sobre *Machine Learning*.

2.1.1.3 *Machine Learning*

Segundo Mitchell (1997), citado por Santos (2005, p. 31),

> a pesquisa em Aprendizado de Máquina (AM) lida com a questão de como construir programas de computadores que possam 'aprender' com a experiência, ou seja, cujo desempenho em determinada tarefa melhora com a experiência. AM é uma subárea de pesquisa de muita importância na Inteligência Artificial (IA), e engloba os estudos de métodos computacionais para a automação da aquisição do conhecimento e para a estruturação e acesso do conhecimento já existente.

Alpaydın (2010, p. 31) aborda algo parecido quando afirma, em uma tradução livre do seu livro em inglês, que:

> Machine Learning é o ato de utilizar programas de computadores para otimizar um desempenho criterioso usando dados de exemplo ou experiência passada. Nós precisamos desse tipo de aprendizado em casos quando não conseguimos escrever diretamente o programa de computador para resolver um certo problema.

Ainda segundo Alpaydin (2020), citado por Pires et al. (2020, p. 26):

> Um sistema baseado em algoritmos de aprendizagem é capaz de, pouco a pouco, melhorar os seus resultados à medida em que vai sendo exposto a dados e consegue acumular experiência a partir deles, algo similar ao que acontece no aprendizado humano.

Em relação ao uso de ferramentas em *Machine Learning*, a estatística e a ciência dos dados são essenciais. Pires et al. (2020, p. 26) sugere:

> Na ciência do Aprendizado de Máquina, a estatística e a ciência de dados estão muito presentes nos processos de inferência construídos a partir de amostras de dados. Elas são ferramentas importantes para se otimizar os algoritmos, uma vez que os dados são a fonte que levará o código a desenvolver sua inteligência artificial. Assim como a qualidade dos livros didáticos influencia o aprendizado humano, a qualidade dos dados é também importante para aprendizado de máquina.

Coppin (2010), citado no artigo de Silva et al. (2012, p.4), também afirma que:

> existem vários métodos de aprendizado de máquina. Entre eles o aprendizado por hábito, que tem como característica o programa aprender por experiência de acordo com o que foi informado anteriormente, mas programa apenas armazena os dados que podem ser classificados, caso ele não conseguir classificar os valores informados método falhará. Há o método de aprendizado por conceito, que analisa todas as hipóteses e demonstra qual é a correta. No método do conceito existe uma subdivisão, que é a 'hipótese mais geral', o que significa que se não existe nenhuma possibilidade correta, o programa achará a que mais se aproxima do correto. Mas estes métodos têm alguns problemas. Por exemplo, nem sempre o usuário quer saber a hipótese correta, e sim a mais comum.

Pires et al. (2020, p. 26) completa dizendo que

> os conhecimentos de ciência e engenharia de computação são utilizados para desenvolver códigos, sensores, máquinas e arquiteturas computacionais através do processo de ETL (extract, transform, load) aplicado aos dados, a fim de criar e alimentar o modelo de aprendizado. Além disso são usados na solução de problemas de otimização, junto à matemática, e para avaliar a inferência dos modelos de ML.

Assim, é correto afirmar que o núcleo dos algoritmos de *Machine Learning* é formado basicamente pelo tipo, qualidade e quantidade de dados coletados. Tendo isso em foco Pires et al.(2020, p. 26) afirma, "eles são diretamente dependentes dos dados utilizados para que se obtenha uma resposta de boa qualidade. Dentro desse contexto, existem vários tipos de algoritmos diferentes e estratégias diferentes de aprendizado".

Dessa forma, faz-se necessário abordar, introdutoriamente, tipos de aprendizado em *Machine Learning.*

2.1.1.4 Tipos de Aprendizado

O emprego de um tipo de aprendizado é definido pelo escopo do domínio do problema e da implementação do algoritmo. Dessa forma, cabe diferenciar tipos de aprendizado.

2.1.1.4.1 Aprendizado Supervisionado

O aprendizado Supervisionado ocorre quando se tenta, através de um conjunto de variáveis independentes, uma variável dependente. Pires et al. (2020, p. 27) explica ao abordar que:

> o algoritmo aprende a partir da definição de um conjunto de variáveis, o domínio, e de seu respectivo conjunto imagem com respeito à função que se deseja assimilar. Basicamente, o programa aprende observando casos em que a resposta é conhecida (rotulada) e fornecida a ele, sendo esses os dados de treino. Assim, detecta-se um padrão para a resposta de acordo com os valores das variáveis de entrada em cada caso e o objetivo do algoritmo é minimizar o erro da saída para casos não conhecidos, ou seja, inputs que não zeram parte do treino do modelo.

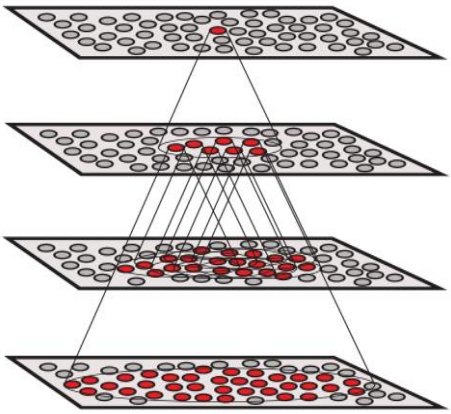
Dessa forma podemos dizer que os dados são anotados de forma prevista. Alpaydin (2020), citado por Pires et al. (2020, p. 27) aborda:

> as inferências de um modelo de Aprendizado Supervisionado são de grande importância para classificações e regressões. Elas tornam possível a previsão de casos futuros não presentes durante o treinamento e a detecção de fraudes a partir da percepção de outliers.

Podem ser citados alguns exemplos para as técnicas de aprendizado supervisionado: Máquinas Kernel, Redes Neurais Artificiais, Árvores de Decisão, Regressão Logística e Regressão Linear.

Na Figura 01 é apresentada uma representação gráfica de aprendizado supervisionado.

Figura 01: Representação gráfica do Aprendizado Supervisionado



Fonte: https://lamfo-unb.github.io/img/tres-tipos-am/f017.png (2022).

Ainda existe um subtipo do Aprendizado Supervisionado conhecido como Aprendizado Semi-supervisionado. Segundo Chapelle et al. (2010), citado por Pires et al. (2020, p. 27),

> Esse tipo de aprendizado é uma forma de aprendizado supervisionado, em que utilizam-se dados rotulados e dados não rotulados. É utilizado em casos em que o ser humano nem sempre consegue classificar de forma eficiente os dados, como no caso de proteínas de três dimensões. Esse tipo de aprendizado pode também ser chamado de aprendizado indutivo, pois consegue inferir rótulos corretos partindo de dados não rotulados.

Um bom exemplo de aplicação do método de aprendizado supervisionado está justamente no reconhecimento de imagens, letras e cores.

Dessa forma, no presente projeto, o algoritmo de reconhecimento facial pode ser classificado em aprendizado supervisionado.

2.1.1.4.2 Aprendizado Não Supervisionado

Ao contrário do Aprendizado Supervisionado que aprende em um ambiente controlado com resultado previsto focando em minimizar erros, o Aprendizado Não Supervisionado possuí um *modus operandi* completamente diferente, nesse método não se busca aprender controlando erros. Nesse caso, através de um ambiente desconhecido, ocorre a identificação de padrões em um determinado banco de dados.

De acordo com Pires et al. (2020, p. 28):

> no aprendizado não supervisionado, nenhuma resposta ou rótulo são fornecidos ao algoritmo, o que limita o escopo de utilização da abordagem. Normalmente, esse método de aprendizado é adequado para detectar desvios em uma distribuição ou grupos de distribuições. Esse aprendizado tem como objetivo encontrar um padrão irreconhecido ou oculto em dados não rotulados.

Dessa forma, pode-se dizer que esse tipo de método foi criado especificamente para auxiliar na área de Ciência dos Dados (*Data Science*). Por exemplo, considere um *site* de compras e vendas que uma de suas funcionalidades é, através do histórico de pesquisa, se moldar conforme o gosto do cliente e, apresentar produtos em que o mesmo estaria mais propenso a comprar.

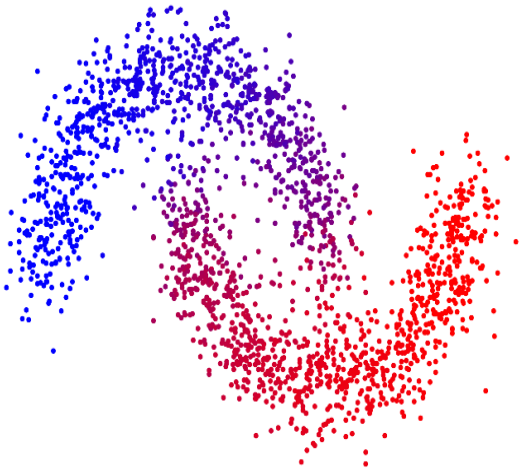
No caso supracitado, pode haver um consumidor que pesquise muito preços de celulares ou marcas de tênis. Tendo em visto isso, apresentar esses produtos de forma rápida na tela inicial mostrando uma promoção especial ou um novo produto, pode levar o aumento de vendas, já que através do perfil do cliente sabe-se do que ele gosta. Claro, para apenas um cliente ou um fluxo mínimo de clientes seria uma tarefa simples. Mas o que aconteceria com um fluxo constante?

Se torna tarefa do computador descobrir e avaliar perfis sem dados estabelecidos. Nesse caso, em decorrência das características especiais, faz-se necessário o emprego do método de Aprendizado Não Supervisionado para achar uma forma informativa uma informação mais detalhada dos dados.

Um exemplo de Inteligências Artificiais que usam esse método é a utilizada nos sites da Amazon e da Netflix. Em ambos os casos, as IA’s automaticamente traçam um perfil dos usuários de acordo com suas pesquisas.

Na Figura 02 é apresentada uma representação gráfica de Aprendizado Não Supervisionado.

Figura 02: Representação gráfica do Aprendizado Não Supervisionado



Fonte: https://lamfo-unb.github.io/img/tres-tipos-am/f008.png (2022)

2.1.1.4.3 Aprendizado por Reforço

Segundo Pires et al.(2020, p. 28),

> nesse tipo de aprendizado, há um agente e um ambiente com o qual ele interage. O objetivo é, inicialmente, fazer o agente realizar ações pseudoaleatórias e puni-lo ou incentivá-lo, através de uma política de recompensa. Uma analogia muito utilizada para aprendizado por reforço é o adestramento de animais, pois a estratégia é parecida, em essência, porém aplicada de forma simulada e com objetivos tão diversos quanto o programador queira. O algoritmo aprende ao otimizar o ganho da recompensa.

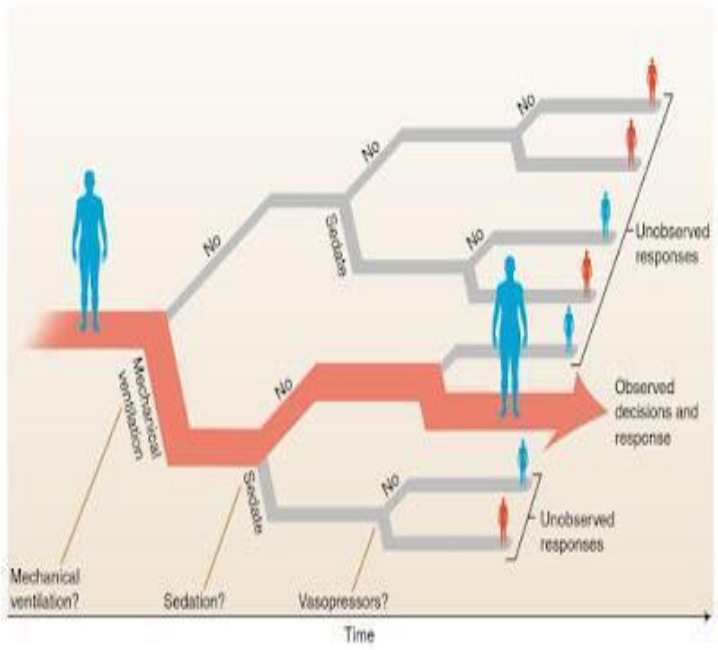
Nessa terceira abordagem o aprendizado da máquina é definido dependendo das circunstâncias em que uma ação será executada. Ou seja, nesse método é definido um conjunto de regras que será moldada conforme a máquina tenta encontrar a melhor situação para obter uma recompensa melhor. Quase como uma rota evolutiva cuja meta é desempenhar uma certa função de formas diferentes até encontrar a resposta ideal.

Muito utilizado em desenvolvimento de jogos e em robótica, a maior vantagem desse método é fazer com que a Inteligência Artificial aprenda em um ambiente complexo e potencialmente incerto. Assim, através de vários casos de tentativas e erros a Inteligência Artificial encontra a melhor situação para maximizar sua recompensa.

Outro benefício é justamente o caso de que com essas simulações é possível gerar infinitas amostras e possibilidades de customização.

A Figura 03 apresenta uma representação de aprendizado por reforço.

Figura 3: Representação gráfica do Aprendizado por Reforço



Fonte: https://www.iaparamedicos.com.br/2019/01/diretrizes-para-o-uso-de-aprendizado.html (2022)

Para fins de revisão teórica, após definições de *Machine Learning*, faz-se necessário também abordar conceitos de redes neurais.

2.1.1.5 Rede Neurais

Pires et al. (2020, p. 30) discorre que “Redes neurais são estruturas computacionais concebidas em analogia aos sistemas nervosos de seres vivos. O conceito de rede neural se baseia no conexionismo, um paradigma de estudo da inteligência e cognição”.
Segundo Fernandes (2005, p. 57),

> é possível se chegar a várias definições do que seja uma Rede Neural Artificial, contudo, as três ‘palavras-chave’: neurônio, arquitetura e aprendizagem, requerem um entendimento, a priori, em qualquer definição de Rede Neural Artificial. O neurônio é a unidade computacional básica de rede em questão; a arquitetura é a estrutura topológica de como os neurônios são conectados; e a aprendizagem é um processo que adapta a rede de modo a computar uma função desejada ou realizar uma tarefa.

Para Lippamann (1997), citado por Fernandes (2005, p. 57),

> as Redes Neurais Artificiais são sistemas físicos que podem adquirir, armazenar e utilizar conhecimentos experimentais, que podem alcançar uma boa performance, devido à sua densa interconexão entre os nós da rede. Elas também são conhecidas por: modelos conexionistas, modelos de processamento paralelo distribuído e sistemas neuromorfológicos.

Ainda segundo Pires et al. (2020, p. 30),

> uma rede neural é composta por camadas de neurônios, para os quais é determinado um conjunto de valores chamados de pesos. As redes neurais são criadas e ensinadas, majoritariamente com aprendizado supervisionado, com o intuito de realizar uma transformação não linear na entrada e chegar-se a resultados em que o erro é aceitável. Para minimizar o erro, o treinamento é feito modicando os pesos até se obterem resultados satisfatórios.

2.1.1.5.1 Características Gerais das Redes Neurais

Segundo Gurney (1997), citado por Fernandes (2005, p. 59),

> uma rede neural artificial é composta por várias unidades de processamento, cujo funcionamento é bastante simples. Essas unidades, geralmente são conectadas por canais de comunicação que estão associados a determinado peso. As unidades fazem operações apenas sobre seus dados locais, que são entradas recebidas pelas suas conexões. O comportamento inteligente de uma Rede Neural Artificial vem das interações entre as unidades de processamento da rede.

Para Filho (1996), citado por Fernandes (2005, p. 59),

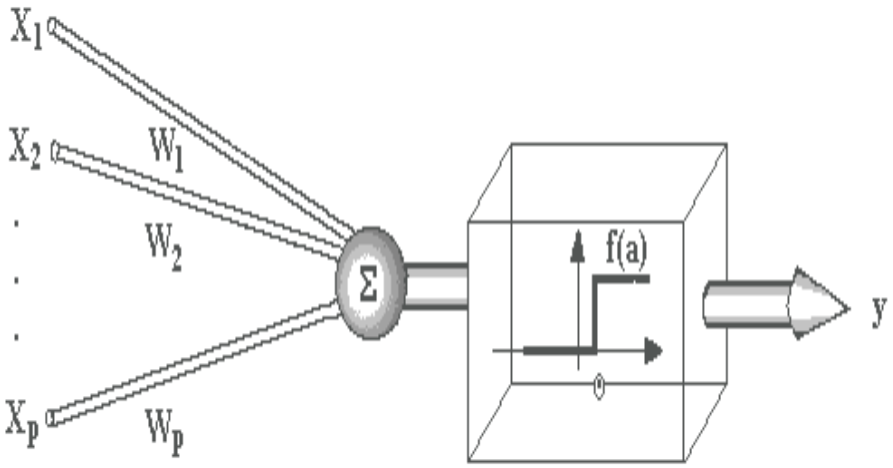
> A operação de uma unidade de processamento, proposta por Mcculloch e Pitts em 1943, pode ser resumida da seguinte maneira: Sinais são apresentados à entrada; Cada sinal é multiplicado por um número, ou peso, que indica a sua influência na saída da unidade; É feita a soma ponderada dos sinais que produz um nível de atividade; Se este nível da atividade exceder um certo limite (*threshold*) a unidade produz uma determinada resposta de saída.

Segundo Fernandes (2005, p. 60), pode-se abordar uma rede neural da seguinte forma:

> Supondo que se tenha os seguintes p sinais de entrada X1, X2, ..., Xp e pesos w1, w2, ..., wp e limitador t; com sinais assumindo valores booleanos (0 ou 1) e pesos valores reais. Neste modelo, o nível de atividade a é dado por:
> a = w1X1 + w2X2 + ... + wpXp
> A saída y é dada por:
> y = 1, se a >= t ou
> y = 0, se a < t.
> A maioria dos modelos de redes neurais possui alguma regra de treinamento, onde os pesos de suas conexões são ajustados de acordo com os padrões apresentados. Em outras palavras, elas aprendem através de exemplos.

Na figura 04 é representado o esquema de unidade de McCulloch e Pitts.

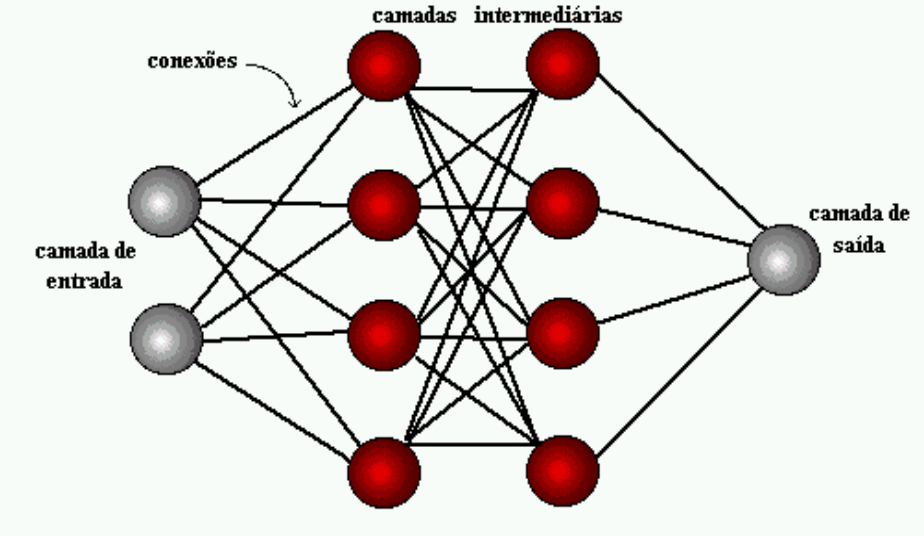
Figura 4: Esquema de unidade de McCulloch e Pitts.



Fonte: https://sites.icmc.usp.br/andre/research/neural/image/mccul.gif (2022)

Segundo Fernandes (2005, p. 61), “arquiteturas de redes neurais são tipicamente organizadas em camadas, com unidades que podem estar conectadas às unidades de camada posterior”, conforme pode ser visualizado na Figura 05.

Figura 05: Camadas de uma Rede Neural Artificial



Fonte: https://sites.icmc.usp.br/andre/research/neural/image/camadas_an.gif (2022)

Para Fernandes (2005, p. 61),

> Usualmente as camadas são classificadas em três grupos:
> Camada de Entrada: onde os padrões são apresentados à rede;
> Camadas Intermediárias ou Escondidas: onde é feita a maior parte do processamento, através das conexões ponderadas; podem ser consideradas como extratoras de características;
> Camada de Saída: onde o resultado final é concluído e apresentado.

Segundo Lippmann (1987), citado por Fernandes (2005, p. 61),

> um neurônio soma rodos os pesos das entradas e passa o resultado para uma função de ativação não-linear. Há três tipos de não-linearidade: limitadores elevados; elementos limiares lógicos e não -linearidades sigmóides.

2.1.1.5.2 Deep Learning (Aprendizado Profundo)

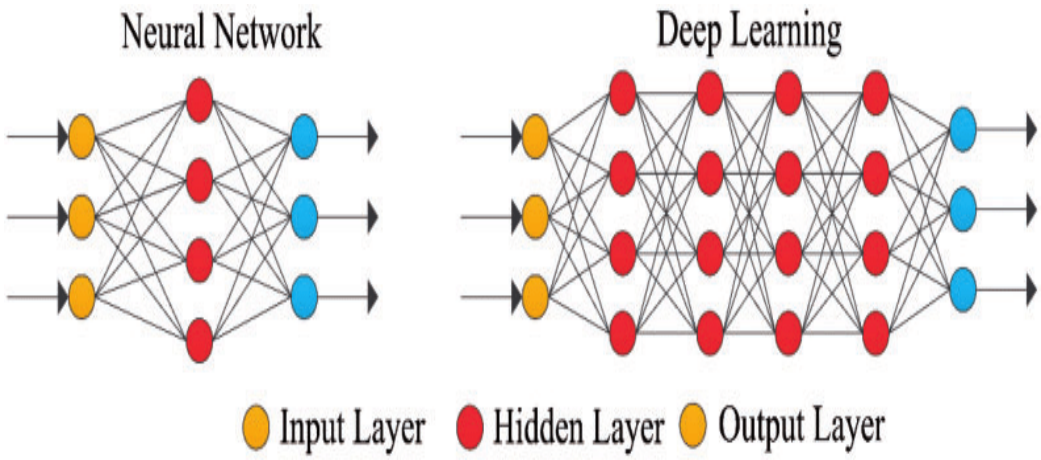
O *Deep Learning* (traduzindo de uma forma livre “Aprendizado Profundo”) pode ser considerado uma subárea do *Machine Learning* e foca em ensinar computadores a se portarem e realizar tarefas como os seres humanos, incluindo reconhecimento de fala e no caso desse projeto, reconhecimento facial.

O grande diferencial do *Deep Learning* para o *Machine Learning* convencional é que no lugar de precisar de uma complexa organização de dados para realizar equações predefinidas para obter o resultado, ele utiliza uma organização de dados mais simples e parâmetros muito mais básicos, “treinando” o computador para aprender sozinho, de modo que ele consiga se

programar de forma adequada para obter um melhor resultado. Geralmente as técnicas utilizadas no *Deep Learning* são baseadas nas habilidades de aprendizado do ser humano, o que a torna muito mais complexa que uma Rede Neural Artificial normal.

A figura 06 mostra a diferença entre duas redes neurais. A da direita é a rede neural profunda, onde possuí um número de camadas escondidas infinitas, muito diferente das redes neurais simples com a sua simplória uma camada escondida ou camada de processamento.

Figura 6: Diferença entre redes neurais simples e profundas



Fonte: https://culturaanalitica.com.br/wp-content/uploads/2018/09/cultura-analitica-redes-neurais-simples-profundas.png (2022)

Pode-se ainda falar que o principal objetivo do *Deep Learning* é ajudar as pessoas a realizar rapidamente tarefas. A Aprendizagem Profunda está sendo muito popular nos dias de hoje, um exemplo de onde podemos encontrar o *Deep Learning* seria no tradutor automático do Google, Drones Automatizados do Amazon e carros autônomos.

2.1.1.5.3 Rede Neural Convolucional (CNN)

De uma forma bem resumida a Rede Neural Convolucional pode ser descrita como um algoritmo de *Deep Learning* que tem como função captar uma imagem de entrada e atribuir valores a transformando em um conjunto de vetores matriciais que a fazem capaz de diferenciar com outras imagens.

Heaton (2017), citado por Pires et al.(2020, p. 32) aborda que:

> as redes neurais convolucionais, também conhecidas como ConvNet, são estruturas de aprendizado de máquina que trabalham com a entrada de maneira matricial. Ao contrário dos algoritmos tradicionais de feedforward, que trabalham com a entrada inteira simultaneamente, as CNN trabalham com apenas uma região por vez. Isso permite um processamento mais eficiente das entradas, analisando informações adicionais, como a posição relativa das entradas. Assim, é largamente utilizado em aplicações que envolvam entradas mais complexas, como processamento de imagens.

Data Science Academy (2022) define a Rede Neural Convolucional como

> um algoritmo de Aprendizado Profundo que pode captar uma imagem de entrada, atribuir importância (pesos e vieses que podem ser aprendidos) a vários aspectos / objetos da imagem e ser capaz de diferenciar um do outro. O pré-processamento exigido em uma ConvNet é muito menor em comparação com outros algoritmos de classificação. Enquanto nos métodos primitivos os filtros são feitos à mão, com treinamento suficiente, as ConvNets têm a capacidade de aprender esses filtros / características.

É importante lembrar que uns dos elementos centrais das ConvNets são seus Kernels, que podem ser descritos como, segundo Pires et al.(2020, p. 32), "matrizes utilizadas para convolução com os dados de entrada de cada camada".

Segundo Goodfellow et al.(2016),

> em aplicações de machine learning, o input é geralmente uma matriz multidimensional de dados, e o kernel é geralmente uma matriz multidimensional de parâmetros que podem se adaptar através do algoritmo de aprendizado. Nos referiremos a esses tensores de matrizes multidimensionais, já que cada elemento do input e do kernel devem ser separados de maneira estrita, geralmente assumimos que essas funções possuam zeros em todos os lugares no conjunto finito de pontos para os quais armazenamos os valores. Isso significa que, na prática, podemos implementar uma soma infinita como uma soma sobre um número finito de elementos da matriz. Finalmente, geralmente usamos convoluções em mais de um eixo por vez. Por exemplo, se usarmos uma imagem bidimensional como nossa entrada, provavelmente também queremos usar uma imagem bidimensional kernel K.

Pires et al. (2020, p. 32), citando o mesmo trabalho de Goodfellow et al. (2016), simplifica quando fala que,

> alguns elementos importantes das ConvNets são os seus kernels, que são matrizes utilizadas para convolução com os dados de entrada de cada camada, e os respectivos stride lengths, que correspondem ao tamanho do passo de cada operação de convolução. Diversos tamanhos de kernel e stride length são utilizados, sempre procurando obter a melhor performance para cada operação específica.

Baseando no fato que I é a matriz de entrada e K o kernel, na Figura 07 está uma representação da equação que descreve a operação da convolução aplicada aos elementos (i; j).

Figura 07: Equação da convolução aplicada dos Elementos

$$S(i,j) = (K * I)(i,j) = \sum_m \sum_n I(i-m, j-n)K(m,n).$$

Fonte: https://www.deeplearningbook.org/contents/convnets.html (2022)

Para Pires et al. (2020, p. 33)

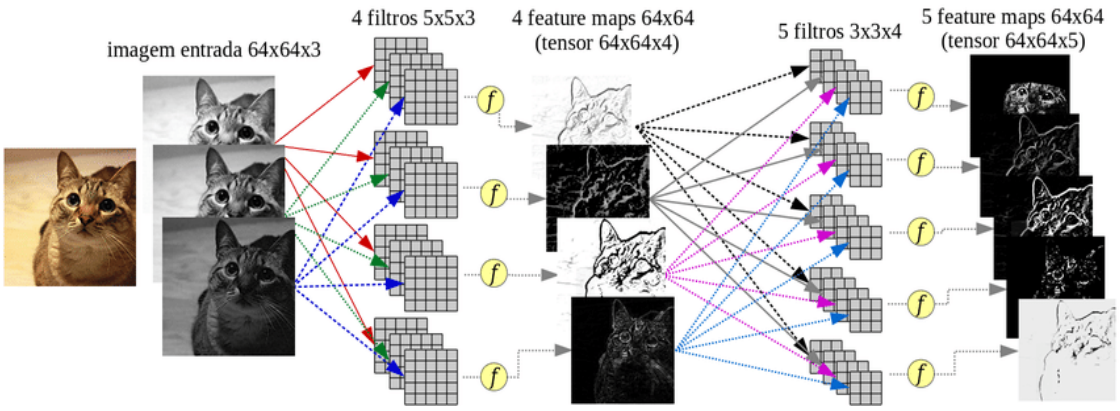
> as redes neurais convolucionais utilizam a ideia de agregação, ou pooling, em que as saídas da operação anterior são condensadas de forma a diminuir o número de parâmetros para as próximas etapas, otimizando o desempenho enquanto mantém informações relevantes a respeito da localização relativa do recurso. Algumas técnicas utilizadas incluem o Max-Pooling, que seleciona o valor máximo de uma dada vizinhança, ou o Pooling L2, que seleciona a raiz quadrada da soma dos quadrados das ativações da região.

Em cada camada convolucional tem-se uma espécie de atribuição para cada neurônio o transformando em uma espécie de filtro imposto na imagem de entrada e cada filtro pode ser considerado uma matriz de pesos. Segundo Pires et al.(2020, p. 33), “Cada fragmento da rede processa e compreende uma característica de dada imagem”.

Ainda, “Características das imagens, como traços verticais e horizontais e características do centro da imagem e das bordas são analisadas por aglomerados de neurônios diferentes da rede, visto a quantidade enorme de variáveis em uma imagem”, conforme abordam os mesmos autores.

Na Figura 08 segue exemplificação de filtros em uma CNN.

Figura 8: Filtros de uma CNN em uma foto de um gato



Fonte:
https://www.researchgate.net/publication/325921947/figure/fig3/AS:640163860475904@1529638366829/Figura-36-Ilustracao-de-duas-camadas-convolucionais-a-primeira-com-4-filtros-5-5.png (2022)

2.1.1.5.4 Embeddings

De uma forma simplificada os *Embeddings* podem ser descritos como uma espécie de representação vetorial contínuas, ou seja, quando se aborda o termo de transformar dados em *Embeddings* nada mais é do que mapear esses dados em uma representação vetorial. *Embeddings* são úteis porque podem reduzir a dimensionalidade de variáveis categóricas e representar categorias de forma significativa no espaço transformado.

2.1.1.6 Biometria Facial

Pode-se definir a Biometria como um estudo de características em forma de análise física ou comportamentais que nos possibilitam identificar uma pessoa de forma única. Já no caso da Biometria Facial ou Reconhecimento Facial, essa análise é usada para confirmar uma pessoa através do rosto.
Segundo Gates (2011),

> em suas aplicações para identificação biométrica, a tecnologia de reconhecimento facial é uma das várias tecnologias que estão sendo desenvolvidas para abordar um problema fundamental preocupação das sociedades modernas: o problema das 'identidades falsas', ou a existência de representações visuais e textuais de indivíduos que circulam independente de seus corpos físicos. Muito antes do desenvolvimento das mídias audiovisuais e bancos de dados eletrônicos, a circulação de informações visuais e textuais representações criaram as condições pelas quais certas classes de seres humanos identidades tornaram-se desvinculadas de sua existência corporal.

No presente trabalho a biometria facial foi utilizada no processo de reconhecimento facial de pessoas, com o fito de identificar possíveis graus de classificação de periculosidade.

Cabe observar que o algoritmo foi desenvolvido pensando em um processo de integração com um drone. O foco foi utilizar o equipamento para identificar um possível rosto

2.1.2 Histórico sobre drones e suas aplicações

Veículo aéreo não tripulado (VANT), também conhecido como Drone é todo e qualquer tipo de aeronave que pode ser controlada nos 3 eixos e que não necessite de pilotos embarcados para ser guiada (DECEA, 2010).

O desenvolvimento dos drones foi inspirado pela Bomba Voadora alemã V1, que era utilizada principalmente em missões onde o risco era muito alto, devido ao espaço aéreo

inimigo ter artilharia antiaérea o que dificultava a passagem de aeronaves grandes e trazia um risco à vida do tripulante.

A partir dessa necessidade e dos avanços tecnológicos foi possível durante a segunda guerra criar uma versão menor da aeronave que posteriormente foi chamada de drone, que começou a ser usada também para espionagem além dos ataques militares.

Além do uso militar, os civis também começaram a utilizar os drones para vários propósitos como fotografias, vigilância, cinegrafia e em vários outros propósitos gerais.

Nos últimos anos essa tecnologia juntamente com as chamadas inteligências artificiais se mostrou revolucionárias pois podem fazer diversas tarefas sejam de uso cotidiano como tirar uma selfie, ou até mesmo ajudar em missões de resgate pois o drone transmite imagens em tempo real, além de poder acessar lugares de difícil acesso, algumas empresas já começaram a testar protótipos para entrega de alimentos ou vigilância (BBC, 2013).

2.1.2.1 Utilização de drones no Brasil

O primeiro VANT do Brasil foi o chamado Gralha Azul, que foi fabricado pela Empresa Brasileira de Veículos Aéreos Não Tripulados (Embravant), em 1996 o Centro de Pesquisas Renato Archer iniciou o Projeto Aurora, que tinha como objetivo desenvolver Drones para as mais diversas áreas, seja de segurança, agricultura ou militar.

A partir da década de 2000, com o avanço da tecnologia portátil os drones ganharam força no mercado que foi quando se iniciou o projeto ARARA (Aeronave de Reconhecimento Autônoma e Remotamente Assistida), pela parceria do Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (ICMC-USP) e a Empresa Brasileira de Pesquisa Agropecuária (Embrapa) para criar em 2005 o primeiro drone asa fixa com tecnologia 100% brasileira e patenteado pela Embrapa.

Em 2007 durante a LAAD (Latin America Aerospace and Defence), a empresa Flight Technologies lançou um VANT tático chamado FS-01 Watchdog, entre 2008 e 2010 em conjunto com o Centro de Estudos Aeronáuticos da Universidade Federal de Minas Gerais (UFMG), lançou a variante FS-01 para atender ao exército Brasileiro.

No final de 2011 que o Brasil ganhou sua primeira aeronave de propulsão elétrica graças à cooperação durante o projeto VANT-SAR entre as empresas AGX, Aeroalcool e Orbisat, financiado pela FINEP (Agência Financiadora de Estudos e Projetos).

Em 2012 a Polícia federal já possuía mais de 15 drones patrulhando as fronteiras e mares costeiros. A partir de 2017 os drones começaram a serem usados massivamente pelos civis para usos como aeromodelismo, vigilância, gravações, selfies e várias outras aplicações.

2.1.2.2 Monitoramento em segurança pública

A segurança pública tem sido um dos assuntos mais debatidos desde o aumento da violência nas grandes capitais, uma das contra medidas tomadas para aparar a situação foi a incorporação da tecnologia inteligente nas metrópoles em pontos estratégicos.

Em 2018 a cidade de Petrópolis, no interior do Rio de Janeiro foi considerado o município mais seguro do Rio de janeiro (PREFEITURA DE PETRÓPOLIS, 2018), pois foram adotadas medidas de segurança aplicados a câmeras com inteligência operacional, além de seu alcance de imagem de 1 quilômetro, foram posicionadas em locais estratégicos 56 câmeras, devido a isso foi possível evitar vários crimes como assaltos a residências, furtos, roubo de carga e até tráfico de drogas.

Porém os avanços não param por aí, em 2019 o governo do Pará passou a investir em recursos da tecnologia de informação e inteligência artificial, e em 2021 as câmeras de monitoramento do sistema de Integração de Registros para Identificação de Suspeitos (Iris), contribuíram para identificação de vários suspeitos em fuga em várias rodovias.

Já os drones beneficiam o setor de segurança pública diante de várias funções como reconhecimento da área de atuação, apoio ao guarda-vidas, análise de risco, monitoramento em tempo real, visualização remota de áreas perigosas e medidas contra a Covid-19 por meio de alto-falantes.

3 IMPLEMENTAÇÃO DO PROTÓTIPO

3.1 TECNOLOGIAS UTILIZADAS NO ALGORITMO DE RECONHECIMENTO FACIAL

3.1.1 Python

A linguagem utilizada para a implementação do código de reconhecimento facial foi Python. Para Pires et al. (2020, p. 36), “Python é uma linguagem de programação de alto nível interpretada. É conhecida por ser extremamente versátil, devido a sua simplicidade e tipagem forte e dinâmica”.

Segundo a apostila “Programa de Educação Tutorial” Grupo PET – ADS (2016),

> Uma das principais características que diferencia a linguagem Python das outras é a legibilidade dos programas escritos. Isto ocorre porque, em outras linguagens, é muito comum o uso excessivo de marcações (ponto ou ponto e vírgula), de marcadores (chaves, colchetes ou parênteses) e de palavras especiais (begin/end), o que torna mais difícil a leitura e compreensão dos programas. Já em Python, o uso desses recursos é reduzido, deixando a linguagem visualmente mais limpa, de fácil compreensão e leitura.

Essa simplicidade foi o motivo essencial da escolha de tal linguagem de programação para o projeto, visto que também possui uma alta compatibilidade com diversas plataformas, além de possuir a existência de importantes ferramentas ou bibliotecas de uso específico para o reconhecimento, visualização de dados e análise como o Numpy e o OpenCV.

A versão utilizada no back-end foi o Python 3.7 por ser mais compatível com as bibliotecas utilizadas e não possuir problemas de conflito, já que inicialmente, na hora da elaboração do código o algoritmo teve que ser refeito várias vezes por falta de compatibilidade.

3.1.2 PyCharm

A IDE escolhida para a construção do programa foi o Pycharm. O Pycharm é uma IDE desenvolvida pela empresa JetBrains e possui aspectos multiplataforma com versões para Windows, Linux e MacOS.

Seu grande diferencial vem justamente do seu depurador gráfico, autocompletamento de código, por ser capaz de fornecer uma análise de código bem apurada e principalmente por facilitar a execução do código em outras máquinas, já que na hora da criação de um novo projeto ele cria uma pasta onde são armazenadas todas as bibliotecas e versões utilizadas do Python, para que, quando o usuário quiser migrar seu projeto para outra máquina não precise baixar todas as bibliotecas novamente.

Sua ampla coleção de plugins, sua versão gratuita poderosa que não fica para trás de qualquer IDE paga e a facilidade de aprendizagem fizeram o PyCharm ser a melhor escolha para o desenvolvimento do sistema proposto.

3.1.3 OpenCV-Python

A “*Open Source Computer Vision Library*” ou simplesmente OpenCV pode ser descrita como a biblioteca mais famosa e utilizada na área computacional. Seu núcleo é voltado

no C++ e pode ser considerada uma biblioteca de código aberto que tem como propósito servir como base ou infraestrutura para a criação de projetos que envolvam a visão computacional.

Segundo Marengoni (2010), “foi idealizada com o objetivo de tornar a visão computacional acessível a usuários e programadores”.

Através dela foi possível acessar coisas importantes para o projeto como webcams de drone e capturar a área de trabalho. Através dela também foi possível ler, editar e converter imagens, assim como padronizar o esquema de cores. O OpenCV-Python já é a versão dessa biblioteca estruturada para Python. Devido ao projeto ser baseado na linguagem Python, foi utilizada essa versão de biblioteca.

3.1.4 Face Recognition

Segundo Simões (2020), “Face Recognition é uma API (Application Programming Interface) de reconhecimento facial, baseada no estado da arte da biblioteca Dlib, desenvolvida em Python e disponibilizada gratuitamente no GitHub do próprio autor”. Foi escolhida para o projeto devido seu treinamento de inteligência artificial poderosa que possibilita a identificação de uma pessoa utilizando uma única foto.

3.1.5 FaceNet

Falcão et al. (2019), “Uma das principais características desse tipo de algoritmo inteligente, é a capacidade de aprender com a experiência”.
Para Simões (2020), “FaceNet é uma rede neural convolucional que mapeia rostos utilizando o conceito de espaços Euclidianos para encontrar as similaridades dos rostos”. Pires et al.(2020, p. 40) aborda que

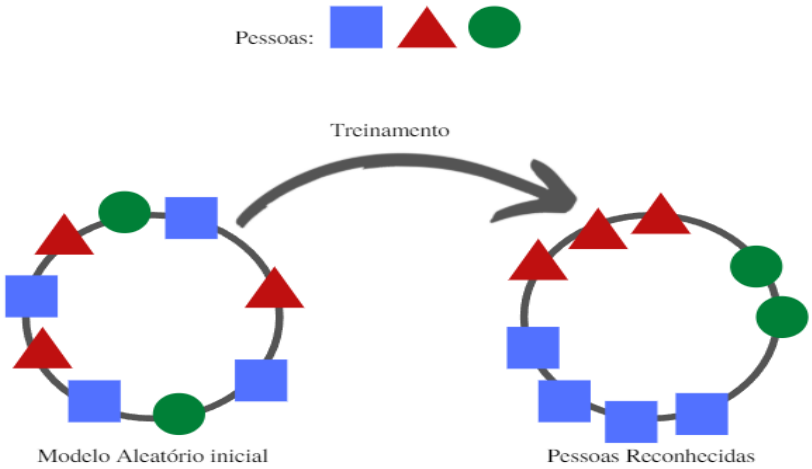
> o modelo FaceNet é uma rede neural convolucional de 426 camadas que extrai as características principais de um rosto. Dada uma imagem de uma pessoa, o Facenet gera um vetor de 128 números, chamado de embedding, que contém informações sobre as características do rosto. Esses embeddings são criados de forma a que rostos semelhantes estejam a uma distância euclidiana menor, enquanto rostos mais distintos possuam uma distância maior.

Segundo Simões (2020), “A função triplet loss do FaceNet agrupa resultados similares de modo que estes permaneçam próximos uns dos outros, e que os diferentes fiquem mais distantes”. Segundo Pires et al. (2020, p. 40):

> O treinamento é realizado através do método triplet loss: dadas três imagens, sendo uma referência (âncora), um exemplo positivo (mesma pessoa), e um exemplo negativo (pessoa diferente), os parâmetros são selecionados de modo a maximizar a distância euclidiana entre exemplos negativos e minimizar a distância entre exemplos positivos. Esse treinamento é realizado em sucessivas iterações até que não haja mais alterações.

Na figura 09 é apresentada uma aplicação da função Triplet Loss do FaceNet

Figura 09: Antes e depois da aplicação da função Triplet Loss do FaceNet



Fonte: http://reports-archive.adm.cs.cmu.edu/anon/anon/usr0/ftp/2016/CMU-CS-16-118.pdf (2022)

Segundo Simões (2020) ao exemplificar o processo, “o FaceNet é aplicado em dois momentos na criação do modelo utilizado no OpenFace. Primeiramente, empregam o modelo pré-treinado do FaceNet para criar um vetor de 128 dimensões que representará um modelo genérico de rosto. Em seguida, utilizarão a função triplet loss para a organização do modelo de modo que ele se torne mais eficiente”.

3.1.6 Numpy

Numpy pode ser considerado a biblioteca principal quando abordamos a computação científica para Python. Possuindo código aberto, sua principal característica se refere ao uso de estrutura de dados, principalmente quando envolve a realização de cálculos e a manipulação de arrays multidimensionais, utilizado em processos de reconhecimento facial.

3.1.7 OS

OS é um módulo nativo que fornece classes para usar funcionalidades variadas dependendo do sistema operacional utilizado, com ele, pode-se fazer coisas como ler, abrir, criar, configurar e editar pastas ou arquivos. Ele foi utilizado para criar uma lista de nomes essencial na identificação visual e registro do avistamento da pessoa cadastrada no banco de imagens.

3.1.8 Geocoder

O Python Geocoder é uma biblioteca de geocodificação simplificada escrita em Python por Denis Carriere. Sua principal aplicação vem justamente do fato de simplificar códigos extensos, conseguindo com uma linha a mesma resposta que se obteria normalmente através de cinco linhas de código. Sua principal função no projeto é a captura da geolocalização no momento em que uma pessoa registrada é reconhecida.

3.1.9 PIL

Com a biblioteca PIL ("*Python Imaging Library*") foi possível adicionar recursos de processamento de imagens ao Python. A principal característica dessa biblioteca vem do fato de oferecer um amplo suporte a formatos de arquivo e recursos de processamento para imagens bem poderoso.

3.1.10 Datetime

É um módulo nativo do Python que fornece as classes para manipulação de data e hora. No projeto sua utilidade vem na parte do registro quando a máquina reconhece uma pessoa registrada.

3.1.11 Tkinter

O pacote tkinter, ou melhor o "*TK interface*" é a interface padrão para o kit de ferramentas do Python. Através dele é possível criar interfaces simples. No caso do projeto esse

pacote foi utilizado justamente para criar um menu em que o usuário poderá escolher em capturar tudo da tela ou ativar diretamente a webcam do computador.

3.3 SISTEMAS OPERACIONAIS

O projeto possui um back-end dividido em dois sistemas operacionais. O primeiro é um sistema com núcleo multiplataforma em Android e iOS que possui a função de conectar um notebook com o drone através de um celular que age como um extensor de sinal, para que o usuário não precise ficar carregando diretamente o notebook.

Já o segundo que é o sistema de reconhecimento em si, foi baseado no sistema operacional Windows, já que é o sistema mais comum. Porém, como o sistema de reconhecimento é baseado no Python, ele possui a possibilidade de ganhar suporte para Linux se fizer necessário.

3.4 DA ARQUITETURA E EXECUÇÃO DO PROJETO

3.4.1 Descrição Geral

O projeto se insere no contexto de reconhecimento de pessoas cadastradas pelo usuário através da captura de tela gerada pela câmera de um drone. O sistema possui grande adaptabilidade, podendo possibilitar, se necessário a captura pela câmera do celular usado como extensor de sinal, pela câmera do próprio notebook ou qualquer outro aplicativo ou vídeo aberto na área de trabalho, como uma câmera de segurança de um estabelecimento ou câmera de uma viatura, por exemplo.

No fluxo principal, o usuário precisa ter uma foto da pessoa a ser identificada dentro da pasta chamada "*imagesAttedence*", no nome da foto deve incluir o número da classe. Existem 3 classes a qual são divididas pelas cores verde, amarelo e vermelho, as quais podem ser usadas como identificação de nível de perigo por exemplo, e deve conter o nome e sobrenome que serão usados no registro de encontro.

Ao executar o aplicativo aparecerá um menu contendo as opções de usar a câmera nativa do notebook, iniciar uma captura da área de trabalho ou fechar a aplicação. Independente da escolha, excluindo é claro fechar a aplicação, abrirá uma tela de captura ao vivo e segundo a opção escolhida, mostrará as imagens da webcam ou uma parte da área de trabalho.

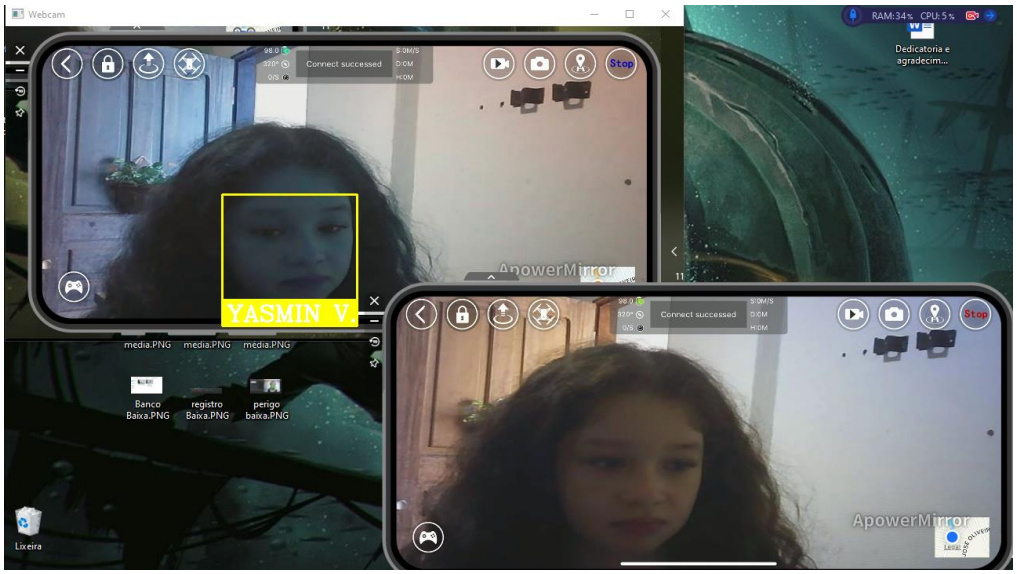
Notasse que tudo que houver na parte capturada como fotos, vídeos ou qualquer outra aplicação será avaliada pelo algoritmo de reconhecimento. Se o sistema identificar uma pessoa cadastrada, uma marcação quadrada em volta do rosto será feita, essa marcação conterá as cores das classes, verde, amarelo ou vermelho, além é claro do nome da pessoa registrada. Possibilitando que o usuário o identifique visualmente na tela de captura.

As Figuras 10, 11 e 12 apresentam as classificações de acordo com o processo de reconhecimento facial realizado pelo algoritmo através do espelhamento da imagem capturada pela câmera do drone.

Figura 10: Reconhecimento Facial com Classificação Verde – Baixo Risco

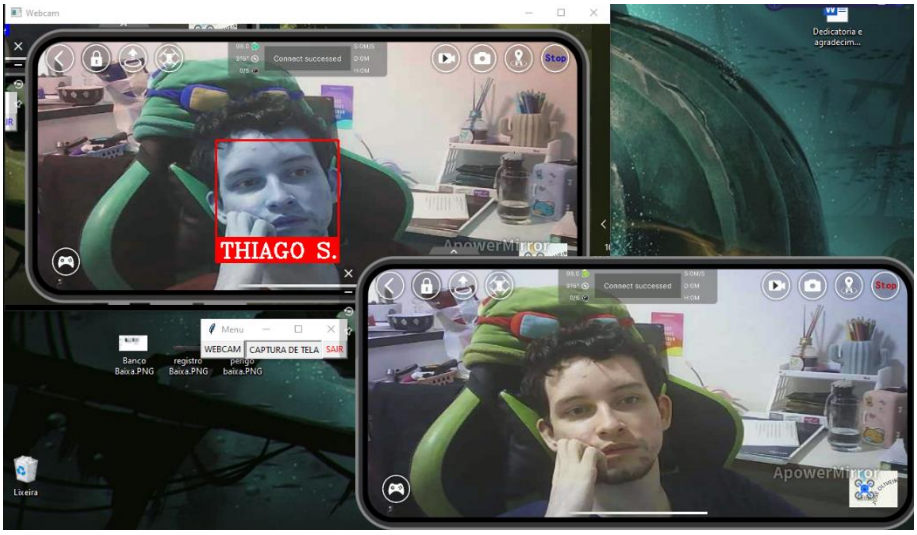
Fonte: Resultados de Testes (2022)

Figura 11: Reconhecimento Facial com Classificação Amarela – Médio Risco



Fonte: Resultados de Testes (2022)

Figura 12: Reconhecimento Facial com Classificação Vermelha – Alto Risco



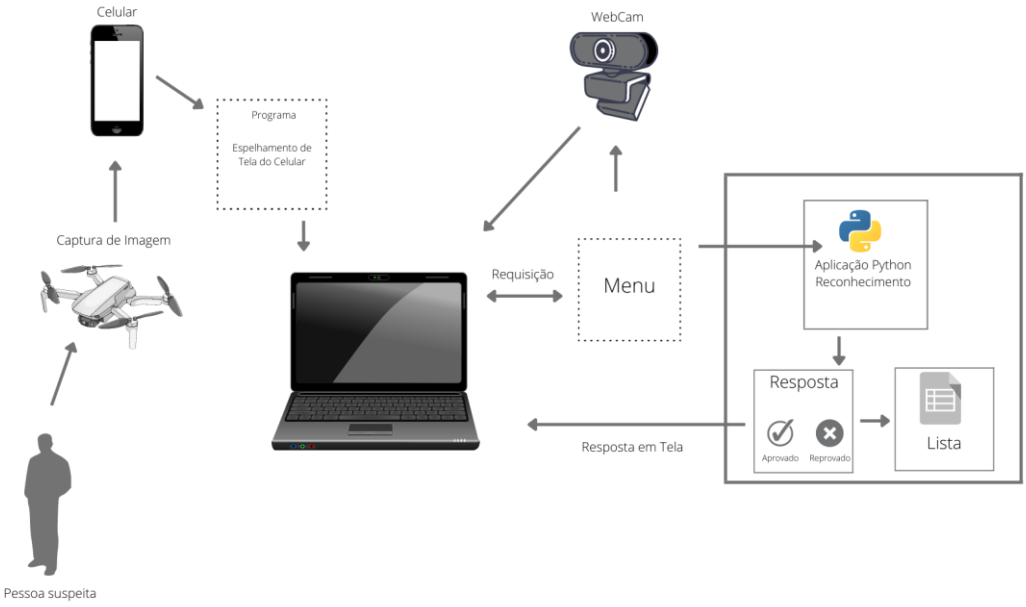
Fonte: Resultados de Testes (2022)

No momento em que uma pessoa cadastrada é reconhecida sua classe, nome, hora e localidade tendo como referencial o notebook será registrada em um arquivo csv que pode ser aberto utilizando o Microsoft Excel, por exemplo. Para parar a captura o usuário deve apertar a letra “q”, nota-se que a tela só poderá ser fechada se a captura parar primeiro. Isso serve como segurança para o usuário contra estranhos tentando fechar a aplicação, por exemplo.

Além disso, usando o drone e o celular como base, o usuário se conectará com a câmera do drone utilizando o celular. Logo após, deverá ser iniciar o aplicativo que espelhará tudo que está rodando nesse aparelho na área de trabalho para que possa ser analisado no programa de reconhecimento facial. O software será responsável por avaliar a tela espelhada e identificar qualquer semelhança entre a foto da pessoa registrada e o rosto capturado pela câmera do drone ou câmera do celular.

Na Figura 13 segue o modelo de integração mais abrangente sobre os componentes do protótipo.

Figura 13: Modelo de integração entre os componentes do protótipo



Fonte: Elaborado pelos autores (2022)

Antes de entrar em questões mais técnicas, cabe ressaltar que em todos os testes realizados o protótipo reconheceu os rostos cadastros de acordo com suas respectivas classificações.

Os testes foram realizados com uso da câmera do drone em solo quanto em voos.

3.4.1.1 Descrição do drone utilizado

De acordo com informações do Amazon (2022), as especificações do drone L900 que foi adquirido para a criação do projeto são:

- L900 Canal: 4;
- Canais Gyro: 6;
- Eixo Motor: Motor Brushless;
- Ângulo elétrico da câmera do ajuste: 90°;
- Ângulo largo da câmera: 120°;
- Frequência da configuração: 2.4ghz;
- Distância de controle remoto: 1000 metros (sem interferência, sem oclusão);
- Tempo de carregamento: 4 horas ou mais;
- Tempo de voo: 28 minutos ou mais;

- Método de transmissão: FPV Figura distância de transmissão: 1000-1200 metros (sem interferência, sem oclusão);

- Resolução da foto: 4096*3072p Resolução de vídeo: 2048*1080p;

- Resolução da foto da câmera inferior: 640*480p;

- Resolução de vídeo da câmera inferior: 1280*720p;

- Modo de gravação de fotos: controle remoto + controle de aplicativo;

- Bateria de controle remoto: bateria de lítio 3.7v 350mah (incluída);

- Quadcopter bateria recarregável: bateria de lítio 7.4v 2200mah (incluída);

- Quadcopter tamanho: 32*32*5cm (desdobrável),13*10*5cm (dobrável);

- Quadcopter peso: 214g.

Obviamente que com um drone com características superiores o protótipo ficaria mais robusto. Entretanto, para o código desenvolvido o drone supracitado atendeu totalmente as expectativas e foi possível implementar, testar e constatar a funcionalidade do protótipo.

Na Figura 11 é apresentado o drone utilizado no projeto.

Figura 14: Drone utilizado no projeto – Vista Superior

Fonte: Registro feito pelos autores (2022)

Figura 15: Drone utilizado no projeto – Vista Frontal

Fonte: Registro feito pelos autores (2022)

3.4.2 Metodologia de classificação de pessoa identificada

Existe um debate amplo sobre a determinação do perigo que um agente apresenta para a incolumidade física e para o patrimônio de outra pessoa. Como o fito de apresentar um modelo que pode ser adaptado e expandido para órgãos de segurança pública, optou-se em três classe de classificação de perigo de um agente identificado.

De acordo com Sato (2012), citando Feinberg, afirma que

> A aplicação do *harm principle* como critério de criminalização de condutas deve ser baseada em generalizações empíricas sobre os efeitos possíveis de ações perigosas sobre interesses tutelados. Aceita que o risco de consequências danosas possa ser comparado ao dano efetivo, admitindo, inclusive as formas de crimes de perigo abstrato. Justifica essa posição pela abertura trazida pelo risco para a possibilidade de danos futuros, para cuja análise será determinante a probabilidade e a gravidade do eventual dano a produzir.
>
> Nos casos em que haja uma probabilidade de dano um pouco maior do que o limite da insignificância, até cerca de 50%, não seria razoável a aplicação da coerção estatal. Sendo assim, pequenas interferências, bem no limite do que se possa considerar dano, não seriam suficientes para uma coerção legal baseada no *harm principle*. Seria uma expressão da máxima, *De minimis non curat lex*. Assim, o próprio *harm principle* já sugere que a intervenção penal sobre o mínimo causará mais dano do que prevenirá. Feinberg vincula essa conclusão a uma filosofia moral utilitarista geral, a qual busca que cidadãos e Legislador maximizem os benefícios e minimizem os danos.
>
> Haveria, portanto, uma proporção inversa entre magnitude e probabilidade do dano: quanto mais provável o dano, menor deve ser sua magnitude para justificar a coerção. Porém, quanto maior o dano, menor sua probabilidade para identificar a necessidade da intervenção penal. O composto de magnitude e probabilidade, segundo Feinberg, constituiria o risco. Além disso, pondera um terceiro fator, o valor da conduta perigosa para o agente, para os terceiros afetados por ela e para a sociedade em geral. Assim, acredita que quanto maior a utilidade social do ato ou atividade em questão, maior deve ser o risco de dano para que sua punição seja justificável.

Considerando os graus de perigos seriam medidos através da probabilidade de dano que o suspeito pode causar em seu ambiente pessoal e social, através de uma pesquisa metódica de seus antecedentes criminais, de maneira mais minuciosa, abordando o próprio perfil do suposto agente, seria possível organizar pelo menos três classificações em relação ao risco apresentado pelo suposto agente.

Dessa forma, pensando em termos de política pública, quanto mais provável o dano, menor deve ser sua magnitude para justificar a coerção e intervenção. Dentro desses três níveis, vermelho se referiria a um sujeito mais provável a causar danos, necessitando, portanto de intervenção imediata. Amarelo apresentaria uma chance geral média e verde uma chance mínima de perigo.

Cabe observar que a metodologia apresentada não é exaustiva. De acordo com a necessidade de emprego do protótipo, novas/outras classes podem ser implementadas, para que o agente público que utilize o equipamento tenha maior suporte para a tomada de decisão em ambientes de crise e/ou de concretização de crimes.

3.4.3 Código do Sistema de Reconhecimento

O procedimento seguido pelo código consiste em duas partes:

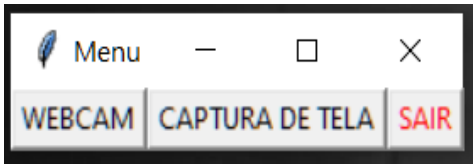
1. faceControl.py: Interface Gráfica do usuário, onde o tipo de execução do programa é executado, consistindo em “WEBCAM”, para a captura direta da webcam do notebook, “CAPTURA DE TELA”, para capturar a área de trabalho e “SAIR” para fechar o programa;

2. Index.py: implementação do código em si com todas as classes, funções e bibliotecas que serão executados pelo sistema.

3.4.3.1 Interface Gráfica do Usuário

A interface gráfica foi programada em *faceControl.py*. Foi utilizada a biblioteca tkinter. O resultado será mostrado logo abaixo na Figura 11:

Figura 16: Menu do Usuário



Fonte: Elaborados pelos Autores (2022).

Ao usuário, é permitido as seguintes ações:

- Utilizar a webcam para o reconhecimento facial;

- Utilizar a captura de tela para reconhecimento facial nos aplicativos ativos na área de trabalho; e

- Fechar aplicativo.

Independente da escolha entre acionar a Webcam ou a Captura da Área de Trabalho, no momento que uma dessas opções for feita por padrão uma série de ações são executadas antes. Essas ações são diversas:

- Importar o diretório de imagens;

- Carregar as imagens que estão no diretório;

- Nomear as Imagens como uma classe;

- Criando uma lista de nomes que será usada para importar as imagens uma por uma na hora da verificação;

- Carregando cada foto utilizando a lista para convertê-las para BGR;

- Usando o Face Recognition para transformar as imagens convertidas em *embedings* que utilizando uma Rede Neural Convolucional comparará esses dados com as imagens capturadas posteriormente para definir se há similaridades.

3.4.3.1.1 Webcam

Pode-se dizer que foi a primeira parte desenvolvida do código, podendo ser considerada a raiz do projeto que mais tarde se tornaria a base para se desenvolver a captura da área de trabalho e consequentemente se conectando com o drone, que é o objetivo final desse sistema.

Quando pelo menu o usuário chama a função WEBCAM a primeira ação que ocorrerá logo após as ações iniciais, será feito através da biblioteca OpenCV. Se constitui em uma checagem para constatar se é possível ligar ou não a Webcam, se a Webcam não ligou se crê que ela não exista ou está com problemas, logo o programa simplesmente fechará. Se por outro lado, for constatado que webcam está ativa então a biblioteca OpenCV começará a ler a imagem gerada.

Lendo a imagem, o OpenCV então fará uma cópia dela e a converterá primeiro para 25% do seu tamanho atual, e depois tornará a imagem colorida em uma imagem com escalas de cinza, para que fique mais fácil quando essa imagem for transformada em *embedings* pelo

Face Recognition. Haverá então uma comparação desses *embedings* com toda a lista de fotos já convertida, e checará uma por uma pra ver ser possuem familiaridades.

Se houver, uma nova função será chamada, essa função trata especificamente do registro de cada foto. No banco de imagem cada foto de uma pessoa cadastrada terá um número de classe, nome e sobrenome. Essa função converterá tudo isso em um array usando como base o caractere “espaço”, e através disso separará o nome e sobrenome da classe. Fora tirar as medidas do rosto que serão tradados na próxima função chamada.

Usando a classe que agora se tornou uma variável solitária definirá uma entre três funções que podem ser descritas como cores, sendo elas o verde, o amarelo e o vermelho.

Definindo a função específica, um retângulo em volta do rosto será desenhado com a cor da função, junto com o nome da pessoa registrada embaixo desse retângulo. Logo após isso, uma outra função será chamada que receberá valores como o nome e o sobrenome, assim como o nome da classe que será atribuído nesse momento.

Essa função primeiramente abrirá o arquivo “avistamento.csv”, depois fará uma checagem se o nome da pessoa registrada está na lista, se não estiver, usará as bibliotecas datatime e geocoder que através do IP da máquina obterá todas as informações necessárias de data, hora e localização. Com o arquivo “avistamento.csv” aberto ela editará o arquivo escrevendo as informações coletadas assim as salvando na lista.

No caso em que exista o nome na lista não haverá edição, essa checagem foi feita justamente para registrar apenas o primeiro avistamento, como se trata de uma captura em tempo real, ou seja, é basicamente um vídeo capturando muitos quadros por segundo, cada quadro pode ser definido como uma imagem isolada que será checada separadamente, sem isso, se uma pessoa registrada ficar na frente por muito tempo da Webcam a lista não pararia de ser reescrita criando muita informação e aumentando o processamento.

Depois que todo esse processo for feito através do OpenCV uma imagem já editada será enviada para a visualização do usuário. Existe também uma função que funciona justamente para parar essa repetição de checagem e visualização, terminando todo o processo ao apertar a letra “q” do teclado. Caso o contrário, mesmo que o usuário tente finalizar ou fechar o processo ele abriria de novo.

Essa opção foi feita justamente para fechar o programa nas primeiras versões do projeto. Foi mantido posteriormente como segurança, ou seja, algum estranho não saberia como fechar o aplicativo, da mesma forma, se houver algum acidente com usuário que o faria fechar o aplicativo por falta de atenção sem apertar a tecla adequada isso seria evitado.

3.4.3.1.2 Captura de Tela

A Captura de Tela pode ser descrita com uma das últimas partes do projeto, sua estrutura é bastante similar com a opção da Webcam, tendo praticamente as mesmas funções e comportamento. A principal diferença está no detalhe que ao iniciar não usará o OpenCV para abrir a Webcam, mas sim usará a biblioteca PIL para criar uma espécie de caixa invisível fixa em formato de uma janela dentro da área de trabalho.

Nesse espaço serão utilizados os recursos da OpenCV quase da mesma maneira que é utilizada a webcam: basicamente ele vai capturar tudo que estiver naquela caixa. Como se trata de uma repetição de captura de quadro a quadro até se pressionar a tecla "q" para interrupção, e como da mesma forma da Webcam, ele vai retornar uma imagem editada para o usuário. O usuário terá a impressão de estar "assistindo" uma gravação como se ele pudesse "espelhar" tudo que estiver ocorrendo naquela caixa invisível na área de trabalho. Dessa forma, qualquer vídeo ou aplicação rodando naquela área será vista como uma imagem separada e será comparada com as fotos registradas a cada repetição do aplicativo.

Então o usuário utilizará uma aplicação para espelhar a tela de um celular conectado com o drone naquela caixa invisível e de forma indireta terá o reconhecimento facial de tudo que for capturado pelo drone.

3.4.3.2 Conteúdos dos códigos do sistema de reconhecimento

O conteúdo dos códigos "*faceControl.py*" e "*index.py*" possuem seu núcleo baseado (e adaptado) no código do curso para reconhecimento facial chamado "*Face Attendance*" de Murtaza Hassan (2020) que por sua vez foi inspirado pelo artigo publicado por Adam Geitgey (2016). O diferencial desse código vem da sua capacidade de reconhecer uma pessoa apenas com uma foto, possibilitando uma economia de tempo e custo computacional em manter um grande banco de dados para o treinamento da inteligência artificial.

Inicialmente esse código foi criado como um exemplo de biometria facial que poderia ser utilizado para um ponto de uma empresa ou marcar presença de um aluno por exemplo. Utilizando esse conceito como base, foram adicionadas diversas novas funcionalidades até chegar em uma aplicação cuja a função não seria apenas marcar a presença de um usuário, mas oferecer uma ampla gama de informações, como o local e a hora em que a pessoa registrada foi vista.

Ainda pode citar que entre as alterações e adições no código, tem-se a criação de um menu, a adição de uma geolocalização mais precisa, a adição da funcionalidade de captura da área de trabalho e três tipos de diferentes classes para o nível de perigo, além de acrescentar o conteúdo da lista que é gerada automaticamente ao encontrar uma pessoa registrada.

3.4.4 Utilização do protótipo em segurança pública

Infelizmente o Acre possui uma deficiência enorme no emprego de tecnologias na segurança pública no embate ao crime, principalmente em uma perspectiva preventiva.

Mesmo após tentar obter algumas informações sobre o emprego de tecnologias pela Secretaria Estadual de Segurança Pública, restou constatado, via informações não documentadas, que os órgãos de segurança pública utilizam câmeras espalhadas pelo Acre, principalmente em Rio Branco.

Entretanto, cabe observar que não existe nem mesmo uma documentação formal sobre a quantidade de câmeras em efetivo funcionamento e suas localizações específicas. Vou comentado por servidores da segurança pública que foram compradas câmeras para uso em serviço de policiais militares. De acordo com a suposta proposta, as câmeras seriam instaladas nas viaturas e nos coletes dos policiais militares.

Cabe observar que nenhuma das informações supracitadas foi confirmada ou negada de maneira oficial. Tal fato já se constituiu em uma limitação do trabalho. Entretanto, não se tem conhecimento do emprego (ou de planejamento de uso no curto prazo) de um protótipo de drone com reconhecimento facial para o auxílio de ações preventivas e repressivas em segurança pública no Acre.

O emprego de tal tecnologia facilitaria a ação do agente público ao passo que fornece a identificação de um suposto agente e sua localização, bem como sua classificação de risco para a realização de possíveis crimes.

Ainda, o emprego de reconhecimento facial através de drones evitaria um confronto inicial entre a autoridade policial e um possível agente delituoso, o que possivelmente iria colaborar para uma maior segurança da autoridade policial e das pessoas existentes no ambiente de identificação de possível agente delituoso.

Dessa forma, mesmo sem informações oficiais, salvo melhor juízo, é notório que o emprego do reconhecimento facial e classificação de supostos agentes utilizando drones, teria inúmeros pontos positivos para a segurança pública e, consequentemente, para o bem-estar da população em geral.

Obviamente que questões como privacidade e resguardo de segurança de identidade são elementos em debate para o emprego de drones em ação de monitoramento de possíveis agentes delituosos. Entretanto, o trabalho se concentrou na proposta da criação do protótipo sem abordar tais debates éticos.

4 CONCLUSÕES

Para uma melhor eficiência nos serviços em segurança pública, faz-se necessário o emprego da maior variedade possível de recursos que possam garantir a segurança do cidadão e a rápida intervenção do Estado na busca de coibir fatos delituosos.

Nesse sentido, o emprego de reconhecimento facial, classificação de indivíduos de acordo com seu grau de periculosidade para a sociedade, bem como de sua localização; através do emprego de drones, é uma forma de contribuir com o aumento de eficiência nos serviços em segurança pública.

O protótipo desenvolvido no presente trabalho empregou recursos de IA e, especialmente de *Machine Learning*, utilizando a linguagem Python para a implementação do algoritmo de reconhecimento facial e classificação de indivíduos com base em imagens geradas por um drone.

Restou constatado que o protótipo atende a proposta inicial do trabalho. Ainda, fica registrado que o projeto pode ser alterado para atender demandas específicas ou de acordo com uma necessidade de determinado órgão da segurança pública do Acre.

O trabalho possui limitações pela falta de informações de bases de dados oficiais, que poderiam auxiliar em um determinado foco para o desenvolvimento do protótipo. Além disso, o uso de recursos de hardware (em especial do drone) não tão robustos dificultou um pouco o desenvolvimento do trabalho, porém não prejudicando sua execução.

Como sugestões para trabalhos futuros, surgem diversas possibilidades: o projeto pode ser alterado e expandido para que o drone siga uma pessoa identificada e localizada de acordo com suas coordenadas geográficas; podem ser implementadas funcionalidades que, dentro das possibilidades, acessem bases de dados oficiais e tenham um maior poder de decisão; e, ainda, pode ser implementado um projeto com emprego de vários drones para uma maior cobertura geográfica, de maneira integrada, auxiliando no mapeamento de uma região e em um possível comportamento delituoso no local.

No mais, o trabalho atendeu sua propositura inicial e, após finalizado, apresentou potencial para ser utilizado, dentro de cada especificidade, pelos órgãos de segurança pública do Estado do Acre.

REFERÊNCIAS

ALPAYDIN, E. **Introduction to machine learning**. Cambridge, Massachusetts: The Mit Press, 2014.

AMAZON. **DRONE L900 5G, GPS, 4K 1.2km Preto : Amazon.com.br: Brinquedos e Jogos**. Disponível em: <https://www.amazon.com.br/DRONE-L900-GPS-1-2km-Preto/dp/B095J3WNKP/ref=asc_df_B095J3WNKP/?tag=googleshopp00-20&linkCode=df0&hvadid=379725971238&hvpos=&hvnetw=g&hvrand=12525848093385558888&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9101739&hvtargid=pla-1327221427438&psc=1>. Acesso em: 2 abr. 2022.

BBC, D. **Amazon testa drones para agilizar entregas**. Disponível em: <https://g1.globo.com/tecnologia/noticia/2013/12/amazon-testa-drones-para-agilizar-entregas.html>. Acesso em: 2 abr. 2022.

BRASIL. **Constituição(1988).Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

DATA SCIENCE ACADEMY. **Deep Learning Book**. Disponível em: <https://www.deeplearningbook.com.br>. Acesso em: 2 abr. 2022.

FALCÃO, J. V. R. et al. REDES NEURAIS DEEP LEARNING COM TENSORFLOW. **RE3C - Revista Eletrônica Científica de Ciência da Computação**, v. 14, n. 1, 18 dez. 2019.

FERNANDES, A. M. DA R. **Inteligência artificial : noções gerais**. Florianópolis: Visual Books, 2005.

FORÇA AÉREA BRASILEIRA, D. C. E. A. **Publicações DECEA**. Disponível em: <https://publicacoes.decea.mil.br/?i=publicacao&id=4510>. Acesso em: 2 abr. 2022.

GATES, K. **Our biometric future : facial recognition technology and the culture of surveillance**. New York: New York University Press, 2011.

GEITGEY, A. **Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning**. Disponível em: <https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78>. Acesso em: 2 abr. 2022.

GOODFELLOW, I.; BENGIO, Y.; COURVILLE, A. **Deep Learning**. Disponível em: <http://www.deeplearningbook.org>. Acesso em: 2 abr. 2022.

GRUPO PET-ADS. **INTRODUÇÃO À PROGRAMAÇÃO COM PYTHON Programa de Educação Tutorial Grupo PET -ADS IFSP -Câmpus São Carlos**. [s.l: s.n.]. Disponível em: <http://antigo.scl.ifsp.edu.br/portal/arquivos/2016.05.04_Apostila_Python_-_PET_ADS_S%C3%A3o_Carlos.pdf>. Acesso em: 2 abr. 2022.

HASSAN, M. **Face Attendance**. Disponível em: <https://www.computervision.zone/courses/face-attendance/>. Acesso em: 2 abr. 2022.

HASSAN, M. **murtazahassan - Overview**. Disponível em: <https://github.com/murtazahassan>. Acesso em: 2 abr. 2022.

HONDA, H.; FACURE, M.; YAOHAO, P. **Os Três Tipos de Aprendizado de Máquina - LAMFO**. Disponível em: <https://lamfo-unb.github.io/2017/07/27/tres-tipos-am/>. Acesso em: 2 abr. 2022.

MARENGONI, M.; STRINGHINI, S. Tutorial: Introdução à Visão Computacional usando OpenCV. **Revista de Informática Teórica e Aplicada**, v. 16, n. 1, p. 125–160, 8 mar. 2010.

PIRES, C. A. S.; LIMA, F. F. D.; SILVA, M. D. A. O. E. **RECONHECIMENTO FACIAL APLICADO A PREVENÇÃO DE FRAUDES**. São Paulo: Universidade de São Paulo, 2020. Disponível em: <https://sites.google.com/view/validface-tcc-project-pcs-usp/>. Acesso em: 2 abr. 2022.

PREFEITURA DE PETRÓPOLIS. **Cidade mais segura do Rio, Petrópolis investe em monitoramento para reduzir ainda mais índices de homicídios**. Disponível em: <https://www.petropolis.rj.gov.br/pmp/index.php/imprensa/noticias/item/9856-cidade-mais-segura-do-rio-petr%C3%B3polis-investe-em-monitoramento-para-reduzir-ainda-mais-%C3%ADndices-de-homic%C3%ADdios.html>.

SANTOS, C. N. DOS. **APRENDIZADO DE MÁQUINA NA IDENTIFICAÇÃO DE SINTAGMAS NOMINAIS: O CASO DO PORTUGUÊS BRASILEIRO**. Rio de Janeiro: INSTITUTO MILITAR DE ENGENHARIA, 2005. Disponível em: <https://www.linguateca.pt/Repositorio/DissertacaoCicero2005.pdf>. Acesso em: 2 abr. 2022.

SATO, C. R. **Crimes de perigo abstrato e a questão da tentativa: limites da antecipação da tutela penal**. São Paulo: Universidade de São Paulo, 2012. Disponível em: <https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15082013-094502/publico/versao_integralCatherine_Ruriko_Sato.pdf>. Acesso em: 2 abr. 2022.

SILVA, B. M. DA; VANDERLINDE, M. **INTELIGÊNCIA ARTIFICIAL, APRENDIZADO DE MÁQUINA**. [s.l: s.n.]. Disponível em: <http://www.ceavi.udesc.br/arquivos/id_submenu/387/brigiane_machado_da_silva___marcos_vanderlinde.pdf>. Acesso em: 2 abr. 2022.

SIMÕES, T. DE S. **UMA ANÁLISE DAS BIBLIOTECAS OPENFACE E FACE RECOGNITION PARA RECONHECIMENTO DE PESSOAS COM OCLUSÃO PARCIAL**. Rio de Janeiro: UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO, 2020. Disponível em: <https://bsi.uniriotec.br/wp-content/uploads/sites/31/2020/07/202005ThaisSouza.pdf>. Acesso em: 2 abr. 2022.

TURING, A. M.; COPELAND, B. J. **The essential Turing : seminal writings in computing, logic, philosophy, artificial intelligence, and artificial life, plus The secrets of Enigma ; [the ideas that gave birth to the computer age]**. Oxford: Clarendon Press, 2010.