Monitoramento de segurança em uma cidade inteligente

GEOVANE GOMES DE SOUSA
JEFERSON RIBEIRO
LUCAS SANTOS
PEDRO LUCAS
MILSON LOUSEIRO LIMA
JORGE HELENO BALDEZ JUNIOR
EWERTON FERREIRA BASTOS

Faculdade Laboro, MA

RESUMO

Ao analisar os vários tipos de monitoramento de segurança em uma cidade inteligente esse artigo visa expor as tecnologias de vídeo monitoramento e reconhecimento facial.

PALAVRAS – CHAVE: Reconhecimento facial. Vídeo monitoramento. Segurança.

ABSTRACT

By analyzing the various types of security monitoring in a smart city, this article aims to expose video surveillance and facial recognition technologies.

KEYWORDS: Facial recognition. Video monitoring. Security.

1. Videomonitoramento na China

É impossível escrever sobre o futuro do combate a criminalidade sem permear a utilização de câmeras de videomonitoramento, 770 milhões de câmeras de circuito de TV(CCTV) estão atualmente em funcionamento no mundo, sendo que 54% dessas estão em funcionamento na China, o país é a melhor referência hoje no assunto e empresas como Huawei, ZTE Corporation, Hangzhou Hikvision Digital Technology, Zhejiang Dahua Technology, Alibaba e outras são responsáveis pela fabricação de câmeras usadas em “cidades inteligentes”(smart cities) pelo mundo todo. Levando em consideração a baixa taxa de criminalidade na China, as estatísticas são de 0,5 mortes por grupo de 100 mil pessoas

em comparação no Brasil, este indicador é de 29,8 por 100 mil, aponta o levantamento do Instituto de Pesquisas Econômicas Aplicada (IPEA) este fator leva o CCTV a ter um apoio massivo da população chinesa 82, 2% são favoráveis a medida é o que diz a pesquisa realizada em 2018 e presente no artigo ***What Explains Popular Support for Government Surveillance in China?*** Escrito pelo professor Zheng Su. Além dessas medidas, o governo chinês também realizou outros investimentos na área seguindo a recomendação do banco mundial que diz que 10% na redução das taxas de homicídios podem levar a um crescimento de 0,7 até 2,9% no PIB. O sistema integrado de vigilância da China, a Skynet, funciona juntamente com o sistema de reconhecimento facial produto da empresa Cloud Walk em colaboração com a Sense Time Group e com a empresa Megvii e funciona com um sistema de reconhecimento facial que opera através de um banco de dados acessado por câmeras presentes em todo o país. Esse sistema "marca" pessoas com comportamento suspeito, o que facilita o despacho rápido de policiais em caso de violações da lei. O sistema até 2019 já tinha auxiliado na captura 10.000 infratores e realiza 1 bilhão de comparações de rosto com a base de dados por ano, apesar disso esse sistema possui limitações, entre elas podemos citar o fato de só conseguir computar 1000 rostos por vez, e o fato da base de dados do sistemas não estar 100% digitalizada o que pode levar a dificuldades no reconhecimento. Porém essas arestas podem ser mitigadas dada a previsão de investimento previsto na área até 2030 que é de 150 bilhões de dólares.

2. Monitoramento na Grande São Luís

A implantação do sistema de videomonitoramento em São Luís foi concluída em Setembro do de 2012 pela empresa Netsolutions avaliado em 19 milhões de reais ele foi empregado em uma época em que os números apontavam uma realidade alarmante para a população ludovicense, a taxa de homicídios havia aumentado em 400% entre 2000 e 2012, o que representava quase o dobro do crescimento nacional no mesmo período, foram 687 mortes violentas em 2012 porém a mudança gradativa veio com o estabelecimento do projeto. O sistema de videomonitoramento da grande São Luís começou com um projeto de 100 câmeras espalhadas pela cidade, com o avanço do projeto essa quantidade foi expandida e hoje conta com 207 câmeras com monitoramento dentro do CIOPS e mais câmeras em operação em unidades estratégicas espalhadas em áreas mais violentas da cidade. Os equipamentos utilizados no projeto são em sua maioria do tipo IP, porém algumas delas também são do modelo analógico, estas são utilizadas no monitoramento da SSP, e do tipo PTZ que são usadas no monitoramento da BR 135. As câmeras possuem uma funcionalidade interativa onde o cidadão pode contactar a central através de um botão localizado no poste. O modelo das câmeras é de uma fabricante escocesa, a Indigovision, que está no mercado desde 1994. A comunicação dos dispositivos com a central de gravação é realizada por meio de fibra óptica. O monitoramento dessas câmeras é realizado por diversas equipes que mantêm a vigilância durante 24 horas e 7 dias da semana dos pontos monitorados, nas saídas da cidade câmeras especiais são utilizadas no rastreio de placas visando o combate ao roubo de carros, de carga e outros delitos relacionados. Recentemente ao sistema também

foram adicionadas câmeras com a capacidade de realizar reconhecimento facial. O acesso às imagens é liberado ao público por meio de solicitação por via da delegacia responsável por investigar o sinistro que motivou a requisição. Com a ajuda do monitoramento, uma queda significativa aconteceu nos índices de criminalidade em São Luís, de 2014 a 2018 os homicídios sofreram uma queda de 63,1% mantendo uma média anual de 299,6 homicídios por ano de 2018 até 2022 segundo dados da SSP. Esses avanços também resultaram em 2017 na retirada de São Luís do ranking das 50 cidades mais violentas do mundo, segundo estudo da organização de sociedade civil mexicana Segurança, Justiça e Paz.

A utilização desse tipo de vigilância abre também espaço para discussões éticas pois levanta o questionamento do quanto as liberdades individuais são prejudicadas por esse avanço. O Maranhão apesar de seguir investindo no videomonitoramento, foram 20 milhões de reais no último ano, ainda não possui aparato legal regulando a sua utilização.

3. O Uso de Inteligência Artificial no Videomonitoramento

O avanço da tecnologia tem trazido diversas inovações para a segurança pública em todo o mundo, e uma das mais promissoras são as câmeras de segurança com inteligência artificial. Esses equipamentos são capazes de reconhecer padrões de comportamento, identificar objetos e pessoas, e enviar alertas em tempo real para as autoridades ou proprietários de imóveis. Com a evolução da tecnologia, espera-se que essas câmeras se tornem ainda mais avançadas e eficazes no futuro.

Em São Luís, capital do estado do Maranhão, a implementação de câmeras de segurança com inteligência artificial já vem sendo estudada. A cidade tem enfrentado uma crescente onda de violência nos últimos 20 anos, o que tem levado as autoridades a buscar soluções mais eficientes para garantir a segurança da população. A utilização de câmeras de segurança com inteligência artificial pode ser uma dessas soluções.

Uma das principais tendências no futuro das câmeras de segurança com inteligência artificial é o uso de algoritmos de aprendizado profundo. Esses algoritmos permitem que as câmeras aprendam com exemplos e sejam capazes de reconhecer padrões e comportamentos com maior precisão. Com o aprendizado profundo, as câmeras de segurança serão capazes de identificar não apenas objetos e pessoas, mas também suas intenções e emoções. Isso tornará a vigilância mais eficiente e eficaz na prevenção de crimes.

Outra tendência importante é a integração das câmeras de segurança com outros dispositivos inteligentes, como sensores de movimento, sistemas de reconhecimento de voz e sistemas de controle de acesso. Com a integração desses dispositivos, as câmeras de segurança poderão ser acionadas automaticamente quando ocorrer uma atividade suspeita.

As câmeras de segurança com inteligência artificial também serão capazes de identificar e prever ameaças com maior rapidez e precisão. Por exemplo, elas poderão detectar e alertar as autoridades sobre comportamentos suspeitos em grandes eventos, como shows ou jogos de futebol, o que pode ajudar a evitar incidentes graves.

As câmeras de inteligência artificial com processadores baseados na arquitetura RISC-V estão emergindo como uma tecnologia promissora que tem o potencial de transformar muitos setores, desde a segurança pública até a indústria automotiva.

Uma das principais vantagens do uso de processadores RISC-V em câmeras de segurança com IA é a capacidade de processamento de dados em tempo real, sendo, muitas das vezes, mais eficiente que o X86 e ARM. Com a IA, as câmeras de segurança precisam ser capazes de analisar grandes quantidades de dados em tempo real e tomar decisões com base nessas informações. Os processadores RISC-V são capazes de processar esses dados em alta velocidade, garantindo que as câmeras possam tomar decisões precisas em tempo real.

A arquitetura RISC-V é particularmente adequada para câmeras de segurança inteligência artificial, porque é altamente escalável. Esses recursos são especialmente importantes em sistemas de segurança, onde as câmeras podem precisar operar continuamente por longos períodos de tempo sem falhas. Além disso, a arquitetura RISC-V está se tornando cada vez mais popular entre as empresas de tecnologia, pois é aberta e livre de royalties, o que significa que os custos de produção para essas câmeras podem diminuir à medida que a demanda aumenta.

Umas das empresas que mais se destacam é a chinesa Kendryte, com seu processador Kendryte K210. O K210 conta dois núcleos, sendo um núcleo de processamento de imagem (DVP) e um núcleo de processamento neural (NPU). O núcleo DVP é responsável pelo processamento de imagens e vídeo, enquanto o núcleo NPU é responsável pelo processamento de redes neurais, permitindo que dispositivos baseados no K210 possam executar tarefas de inteligência artificial em tempo real.

No entanto, é importante destacar que o uso de câmeras de segurança com inteligência artificial também levanta questões éticas e de privacidade. As câmeras poderão coletar grandes quantidades de dados pessoais, como imagens faciais e padrões de comportamento, e é necessário garantir que esses dados sejam protegidos e utilizados de forma responsável. Além disso, a utilização desses sistemas deve ser regulamentada para garantir que não sejam usados para violar os direitos dos indivíduos ou para fins discriminatórios.

É importante envolver a população e a sociedade civil no debate sobre a utilização de câmeras de segurança com inteligência artificial, para que haja transparência e participação no processo de implementação desses sistemas.

Além disso, é necessário investir em capacitação e treinamento para os profissionais que irão operar as câmeras de segurança com inteligência artificial, para que saibam utilizar esses equipamentos de forma eficiente e responsável. É importante que as autoridades estabeleçam protocolos claros para a utilização desses sistemas, garantindo que os dados coletados sejam utilizados apenas para fins legítimos.

4. Reconhecimento Facial Nos Dias Atuais.

Criada nos anos 1960, a tecnologia que usa computadores e algoritmos para reconhecer rostos humanos ganhou escala há pelo menos uma década, muito graças ao avanço das redes sociais e da internet. Com milhares de pessoas disponibilizando voluntariamente suas fotos na internet, existe hoje um banco de dados com bilhões de imagens que servem para treinar redes de inteligência artificial a detectar e reconhecer rostos.

As possibilidades são inúmeras, e você certamente já se deparou com alguma delas no dia a dia — segundo o levantamento da Surfshark, 92% dos países na América do Sul usam reconhecimento facial, a maior porcentagem entre os continentes. Do seu filtro favorito no Instagram ao desbloqueio de celulares, até a identificação em aeroportos (o Brasil está entre os países que têm um sistema automatizado de leitura de passaportes), o reconhecimento facial é usado em algum nível. Há também casos mais "avançados", como o do homem chinês que foi sequestrado quando criança e, graças à tecnologia de reconhecimento facial, utilizada nas buscas, reencontrou os pais depois de 32 anos; ou do carnaval de Salvador de 2020, no qual câmeras de segurança identificaram e ajudaram a capturar 42 foragidos da Justiça.

"Passamos de uma fase de detecção, que era o que tínhamos com as câmeras digitais antigas que viam um sorriso e tiravam a foto, para a de reconhecimento propriamente dito, de saber de quem é aquele rosto", explica o especialista em tecnologias emergentes Diogo Cortiz, professor da Pontifícia Universidade Católica de São Paulo (PUC-SP). "Isso está muito atrelado à inteligência artificial aplicada ao processamento e tratamento de imagens."

O caso mais comum de utilização da tecnologia de reconhecimento facial é sua aplicação em aparelhos eletrônicos, como celulares, computadores e câmeras fotográficas ou filmadoras. Smartphones modernos, como é o caso do Iphone X, já contam com processos de segurança ligados ao reconhecimento da geometria facial dos usuários. O equipamento utiliza a sua câmera para a captura do padrão do rosto e automaticamente coloca os dados em um banco de dados, sendo acessado toda vez que for solicitado o desbloqueio da tela. A tecnologia utilizada nesses aparelhos já alcançou uma maturidade, fato comprovado pela identificação do usuário mesmo com o uso de chapéu, maquiagem, óculos ou mudança no corte de cabelo. Assim como celulares, computadores já utilizam a captura de padrões faciais para liberar o acesso de usuários a programas ou arquivos, garantindo a segurança de dados.

Facial Recognition Technology (FRT) é a habilidade que softwares têm de identificar rostos humanos a partir de fotos ou vídeos. Ao utilizar diferentes bancos de dados, é possível processar as imagens dos rostos e catalogá-las com os detalhes de cada indivíduo, sendo que os dados processados podem ser utilizados para diferentes propósitos. Simultaneamente ao desenvolvimento dessa técnica, com o avanço da internet, existe uma crescente coleta de dados pessoais, que se transforma em uma interconexão entre

diferentes bancos de dados, realizando o cruzamento de informações de um indivíduo e criando um perfil para cada usuário.

O sistema eletrônico de vigilância na China utiliza a tecnologia de reconhecimento facial para identificar crianças desaparecidas. O governo chinês, em conjunto com empresas de tecnologia, criou um software que compara as imagens e 'envelhece' a criança através de um sistema que tem como objetivo prever a aparência correspondente ao tempo de seu desaparecimento. De acordo com o jornal El País, a plataforma é eficiente em 96% dos casos, sendo que em três anos a tecnologia possibilitou que fossem encontradas 6,7 mil crianças.

Na Índia, a organização Bachpan Bachao Andolan (BBA) desenvolveu um sistema de reconhecimento facial que auxilia o processo de comparação do TrackChild, um banco de dados online criado pelo Ministério de Desenvolvimento das Crianças e das Mulheres no qual são postadas fotos de crianças desaparecidas. Após sua implementação, o Software encontrou mais de 2.930 crianças.

Já no Brasil, a tecnologia de reconhecimento facial está auxiliando o Rio de Janeiro a encontrar criminosos foragidos. Após quatro meses de teste, as câmeras instaladas nas regiões de Copacabana e no Maracanã já possibilitaram a prisão de 63 pessoas. Na Bahia, o Sistema de Reconhecimento Facial da Secretaria de Segurança Pública da Bahia, possibilitou a captura de 93º indivíduos foragidos.

5. As melhorias nos Softwares de Reconhecimento Facial.

Os softwares de reconhecimento facial têm evoluído significativamente nos últimos anos, com várias melhorias importantes. Algumas das principais melhorias nos softwares de reconhecimento facial incluem:

Precisão: A precisão dos algoritmos de reconhecimento facial tem melhorado consideravelmente, com taxas de acerto cada vez mais altas. Isso é resultado do aprimoramento dos algoritmos de aprendizado de máquina e da disponibilidade de conjuntos de dados de treinamento mais abrangentes e diversificados.

Velocidade: Os softwares de reconhecimento facial estão se tornando mais rápidos em processar grandes volumes de imagens em tempo real, o que é crucial para aplicações em tempo real, como vigilância e autenticação de usuários.

Robustez: Os algoritmos de reconhecimento facial estão se tornando mais robus-

tos em relação a variações nas condições de iluminação, pose facial, expressões faciais e envelhecimento. Isso permite um desempenho mais consistente em diferentes ambientes e situações.

Confiabilidade: As melhorias na confiabilidade dos softwares de reconhecimento facial têm sido alcançadas através da redução de falsos positivos (quando uma pessoa é incorretamente identificada como outra) e falsos negativos (quando uma pessoa não é identificada corretamente). Isso tem sido alcançado por meio de técnicas mais avançadas, como redes neurais convolucionais e redes neurais profundas.

Privacidade: A preocupação com a privacidade tem sido abordada em algumas melhorias recentes nos softwares de reconhecimento facial. Por exemplo, técnicas de anonimidade de dados, criptografia e controle de acesso têm sido implementadas para proteger a privacidade dos indivíduos e garantir o uso ético e legal da tecnologia.

Viés e diversidade: outra área de melhoria nos softwares de reconhecimento facial é a redução de viés e aumento da diversidade nos conjuntos de dados de treinamento. Viés e falta de diversidade podem levar a resultados discriminatórios, especialmente em relação a gênero, raça e idade. Portanto, os esforços para tornar os algoritmos de reconhecimento facial mais justos e equitativos são uma área importante de pesquisa e desenvolvimento.

6. Biblioteca de reconhecimento facial de código aberto.

- **OpenBR**

O OpenBR (Open Biometrics) é uma biblioteca de código aberto desenvolvida pelo Laboratório de Pesquisa em Biometria (Biometrics Research Lab) da Universidade de Notre Dame, nos Estados Unidos. Ele fornece uma variedade de algoritmos e ferramentas para tarefas relacionadas a biometria, incluindo reconhecimento facial, reconhecimento de impressão digital e reconhecimento de íris. O OpenBR oferece uma interface de programação de aplicativos (API) para acessar funcionalidades avançadas de processamento de imagem, como detecção de rosto, extração de características faciais e correspondência de faces. É uma biblioteca altamente flexível e personalizável, permitindo que os desenvolvedores ajustem os parâmetros dos algoritmos e integrem o reconhecimento facial em suas aplicações de acordo com suas necessidades específicas.

- **OpenFace**

O OpenFace é outra biblioteca de código aberto para reconhecimento facial desenvolvida pelo Carnegie Mellon University Robotics Institute, nos Estados Unidos. Ele oferece uma implementação eficiente e fácil de usar de algoritmos de visão computacional e aprendizado de máquina para tarefas de reconhecimento facial, como detecção de rosto, extração de características faciais e reconhecimento de faces. O OpenFace é conhecido por sua precisão e desempenho em aplicações de reconhecimento facial em tempo real e é amplamente utilizado em projetos de pesquisa e aplicativos práticos. Ele também oferece suporte a várias arquiteturas de redes neurais convolucionais pré-treinadas, como o modelo de representação de face DeepFace, que pode ser utilizado para tarefas de reconhecimento facial.

Ambas as bibliotecas são de código aberto, o que significa que seu código-fonte está disponível gratuitamente e pode ser modificado e distribuído pela comunidade de desenvolvedores. Elas são usadas em uma ampla gama de aplicações, incluindo segurança, autenticação biométrica, análise de vídeo, entre outras. No entanto, é importante respeitar as normas de privacidade e ética ao usar tecnologias de reconhecimento facial, garantindo o uso adequado e legal dos dados de identificação pessoal.

Em resumo, os softwares de reconhecimento facial têm evoluído consideravelmente nos últimos anos, com melhorias na precisão, velocidade, robustez, confiabilidade, privacidade, e na redução de viés e aumento da diversidade. Essas melhorias ampliam o potencial de aplicação da tecnologia de reconhecimento facial em diversas áreas, mas também têm levantado questões éticas e de privacidade que precisam ser cuidadosamente abordadas

REFERÊNCIAS

OS DADOS DA VIOLÊNCIA E DA CRIMINALIDADE EM SÃO LUÍS, Organizadores: LAURA REGINA CARNEIRO MARLANA PORTILHO RODRIGUES

EDUARDO CELESTINO CORDEIRO

Elaboradores: ANA PAULA LACERDA

EDUARDO FRAGOSO

JOÃO EDUARDO COUTINHO MELO

ROSEANE SANTOS

Setembro de 2019

Information technology as a means of combating crime in China, Nadezhda Slivinskaya (MGIMO)

Vitaly Vasyukov (MGIMO)

Maio, 2021

What Explains Popular Support for Government Surveillance in China?

Zheng Su, Xu Xu, Xun Cao

Dezembro 2021

A VIABILIDADE DO VIDEOMONITORAMENTO PARA AUXILIAR NO SERVIÇO

DE GUARDA-VIDAS NA PRAIA DO CALHAU

FELIPE DO NASCIMENTO PEREIRA, 2019

Exporting Chinese surveillance: the security risks of 'smart cities'
James Kynge in Hong Kong, Valerie Hopkins in Belgrade, Helen Warrell in London and Kathrin Hille in Taipei JUNE 9 2021

This state-backed AI unicorn has helped Chinese police arrest 10,000 criminals
Iris Deng, Março, 2019 (https://www.scmp.com/tech/start-ups/article/3003686/state-backed-ai-unicorn-has-helped-chinese-police-arrest-10000)

3rd International Conference on Computer Science and Computational Intelligence 2018
Face Recognition Using Modified OpenFace Kevin Santoso, Gede Putra Kusuma* Computer Science Department, BINUS Graduate Program – Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia, 11480