UNIVERSIDADE DE SÃO PAULO
ESCOLA POLITÉCNICA
DEPARTAMENTO DE ENGENHARIA DE COMPUTAÇÃO E SISTEMAS DIGITAIS

MANOEL AUGUSTO DA SILVA JUNIOR

Utilização eficiente em larga escala de reconhecimento facial para análise preditiva de segurança em cidades inteligentes

São Paulo
2019

MANOEL AUGUSTO DA SILVA JUNIOR

Utilização eficiente em larga escala de reconhecimento facial para análise preditiva de segurança em cidades inteligentes

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para a obtenção do título de Mestre em Ciências.

Área de Concentração: Engenharia de Computação

Orientador: Prof. Dr. José Sidnei Colombo Martini

São Paulo

2019

Este exemplar foi revisado e alterado em relação à versão original, sob responsabilidade única do autor e com a anuência de seu orientador.

São Paulo, ... de .....de 20

Assinatura do autor

Assinatura do orientador

Catalogação na publicação

Serviço de Biblioteca e Documentação

Escola Politécnica da Universidade de São Paulo

Silva Junior, Manoel Augusto

Utilização eficiente em larga escala de reconhecimento facial para análise preditiva de segurança em cidades inteligentes / Manoel Augusto Silva Junior ; orientador, José Sidnei Colombo Martini – versão corr. – São Paulo, 2019.

115 f. : il.

Dissertação (Mestrado em Ciências) – Departamento de Engenharia de Computação e Sistemas Digitais, Escola Politécnica, Universidade de São Paulo.

1. Inteligência Artificial. 2. Universidade de São Paulo. 3. Escola Politécnica. I. Martini, José Sidnei Colombo, orient. II. Título.

MANOEL AUGUSTO DA SILVA JUNIOR

Utilização eficiente em larga escala de reconhecimento facial para análise preditiva de segurança em cidades inteligentes

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para a obtenção do título de Mestre em Ciências.

São Paulo

2019

Nome: SILVA JUNIOR, Manoel Augusto.

Título: Utilização eficiente em larga escala de reconhecimento facial para análise preditiva de segurança em cidades inteligentes.

Dissertação apresentada à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Ciências.

Aprovado em:

Banca Examinadora

Prof. Dr. _____

Instituição: _____

Julgamento: _____

Prof. Dr. _____

Instituição: _____

Julgamento: _____

Prof. Dr. _____

Instituição: _____

Julgamento: _____

Dedico esta dissertação de mestrado ao Gabriel e à Isabella, meus filhos, e à Zuleica, minha esposa, que estiveram incondicionalmente ao meu lado, me apoiando e incentivando em todos os momentos.

AGRADECIMENTOS

Ao Prof. Dr. José Sidnei Colombo Martini, pelo incentivo em todos os momentos e por generosidade de me permitir aprender com a sua imensa sabedoria, a sua dedicação comigo como mentor e amigo foram imprescindíveis para a construção deste trabalho.

À minha mãe Maria Aparecida, por sempre ter me ajudado incansavelmente desde muito cedo em minha dedicação aos estudos, fazendo tudo que estivesse ao seu alcance para que eu pudesse atingir meus objetivos.

Ao meu pai Manoel Augusto, quem me mostrou um computador pela primeira vez e despertou em mim o interesse por esta incrível máquina.

À Escola Politécnica da Universidade de São Paulo, por ter se tornado uma segunda casa, onde pude aprender muito, conhecer pessoas brilhantes e fazer grandes amigos.

RESUMO

SILVA JUNIOR, M. A. **Utilização eficiente em larga escala de reconhecimento facial para análise preditiva de segurança em cidades inteligentes**. 2019. 115 f. Dissertação (Mestrado em Ciências) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2019.

As cidades concentram mais de 50% da população mundial e a segurança dessas pessoas é um dos fatores mais importantes atualmente. A gestão deste tema é complexa e exige um grande esforço e, em muitos casos, é feita de maneira ineficiente e baseada em decisões empíricas e opiniões. O conceito que vem sendo chamado de “cidades inteligentes” é uma tendência mundial que congrega diversas práticas de ações sustentáveis utilizando soluções tecnológicas como instrumento para tornar as cidades mais eficientes, otimizando vários aspectos da vida urbana e melhorando a qualidade de vida dos habitantes. À medida em que as cidades vão se tornado mais inteligentes, sobressai a necessidade de evoluir também a forma de garantir que todos os cidadãos desta mesma cidade estejam seguros, e isto, quando feito de uma forma eficiente, consome racionalmente recursos que são caros e limitados. Esse trabalho propõe a análise sistemática para a Utilização Eficiente em Larga Escala de Reconhecimento Facial para Análise Preditiva de Segurança em Cidades Inteligentes, baseado em informações históricas previamente coletadas e outras que serão obtidas continuamente, em tempo real. O objetivo desse estudo é detalhar como ter a tecnologia como aliada para aproximar as pessoas, envolvendo-as no compartilhamento de informações que ao serem processadas através de um modelo matemático apresentarão um indicador de periculosidade de certa coordenada geográfica em um determinado instante. A utilização correta de reconhecimento facial permite aumentar a capacidade de monitoramento dos espaços públicos, tornando mais eficientes as atividades de proteção aos cidadãos. Neste estudo serão abordados os desafios tecnológicos relevantes para a utilização de diferentes algoritmos para o acompanhamento em tempo real de câmeras e em larga escala. É necessário um conjunto de boas práticas de arquitetura e desenvolvimento de software para construir e manter um sistema seguro para os usuários, minimizando possíveis prejuízos financeiros e espera-se que com a adoção de um padrão elevado de qualidade em segurança possam ser atendidos os mais altos níveis de requisitos funcionais e não funcionais necessários para operações com esta criticidade.

Palavras-chave: Inteligência Artificial. Visão Computacional. Reconhecimento Facial. Cidades Inteligentes.

ABSTRACT

Cities are home to more than 50% of the world's population and the safety of these people is one of the most important factors today. The management of this topic is complex and requires a great deal of effort and, in many cases, is done inefficiently and based on empirical decisions and opinions. The concept that is being called “smart cities” is a worldwide trend that brings together diverse sustainable practices using technological solutions as an instrument to make cities more efficient, optimizing various aspects of urban life and improving the quality of life of their inhabitants. As cities become smarter, there is also a need to develop ways to ensure that all citizens of the city are safe, and this, when done in an efficient way, consume expensive and limited resources more rationally. This work proposes a systematic analysis for the Efficient Use in Large Scale Facial Recognition for Predictive Analysis of Safety in Smart Cities, based on historical information previously collected and others that will be obtained continuously, in real time. The objective of this study is to detail how to have technology as an ally to approach people, involving them in the sharing of information that, when processed through a mathematical model, will present a hazard indicator of a certain geographic coordinate at a given instant. The correct use of facial recognition allows increasing the capacity of monitoring public spaces, making citizen protection more efficient. This study will address the technological challenges relevant to the use of different algorithms for real-time monitoring of cameras and on a large scale. A set of good architecture and software development practices is required to build and maintain a secure system for users, minimizing potential financial losses, and it is expected that by adopting a high standard of security quality, the highest standards of functional and non-functional requirements for such critical operations can be met.

Keywords: Artificial Intelligence. Computer Vision. Facial Recognition. Smart Cities.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADRO

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANEEL	Agência Nacional de Energia Elétrica
CISC	Complex Instruction Set Computing
CNN	Convolutional Neural Network
CPU	Central Processing Unit
CSRF	Cross-Site Request Forgery
CUASO	Cidade Universitária Armando de Salles Oliveira
GPU	Graphics Processing Unit
IACP	International Association of Chiefs of Polices
INFOCRIM	Informações criminais
LCA	Linear Discriminant Analysis
ONG	Organização não governamental
PCA	Principal Component Analysis
RDO	Registro Digital de Ocorrências
RISC	Reduced Instruction Set Computing
SIGINURB	Sistema Integrado de Gestão da Infraestrutura Urbana
SLA	Service Level Agreement
SVM	Suport Vector Machine
TIC	Tecnologias da Informação e Comunicações
UCRS	Uniform Crime Report System
XSS	Cross-Site Script

SUMÁRIO

1 INTRODUÇÃO

Desde a antiguidade as cidades sempre foram muito importantes para a humanidade, pois concentravam o comércio, o conhecimento para educação e diversos lugares de contato para o relacionamento humano, como lazer, religião e política.

De acordo com a ONU Habitat, a população urbana global, que em 2014 era de 54%, deve crescer para 70%, em 2050 (HABITAT III).

Um dos pontos que mais contribuiu para o êxodo rural foi a Automação Agrícola, permitindo uma eficiência muito maior na produção de alimentos com um número menor de pessoas envolvidas, cultivando áreas maiores de forma mecanizada e a utilização de melhores insumos agrícolas (sementes, defensivos, vitaminas) aumentaram significativamente a produtividade rural, deixando profissionais de baixa qualificação técnica sem trabalho e os obrigando a buscar novas oportunidades nas cidades.

Esse processo rápido de urbanização tem trazido grandes desafios para os gestores de cidades. Problemas relacionados ao tráfego, segurança, educação, saúde, consumo de água e energia, entre outros, nos últimos anos estão se tornando mais difíceis de serem administrados. As tecnologias da informação e comunicações (TIC) podem ter um papel importante no auxílio do monitoramento, controle e tomada de decisões diante de tais problemas.

O conceito que vem sendo chamado de Cidades Inteligentes, termo criado pela IBM (Smart Cities) é uma tendência mundial relativa ao emprego de práticas de sustentabilidade e o uso de soluções intensivas de TIC como instrumentos para tornar cidades inteligentes otimizando vários aspectos da vida urbana.

A ONG Social Progress Imperative (2018) divulgou um ranking da qualidade de vida em 146 países, referente ao índice de Progresso Social. Entre os dados analisados, o principal é a segurança pessoal, item que o Brasil aparece como o 22º país mais inseguro do mundo.

Nos últimos anos, com a tecnologia sendo usada intensivamente, as cidades têm se tornado mais inteligentes, e os computadores podem auxiliar em diversos tipos de tarefas cotidianas. Aliado a isto há o aumento do uso de sistemas dotados de Inteligência Artificial permitindo assim que se possa avançar

sobre tarefas complexas, repetitivas e de alto custo caso fossem executadas em larga escala por seres humanos.

Considerando esse cenário, surgiu a iniciativa de utilizar a tecnologia para contribuir na otimização do processo de tomada de decisão, monitoramento e controle realizado pelos gestores de segurança pública, para monitorar as câmeras de segurança em larga escala de uma cidade inteligente e estimar preditivamente os possíveis indícios de criminalidade em uma determinada área. Com estas informações calculadas é possível otimizar o planejamento das equipes de segurança, buscando reduzir os níveis de periculosidade e melhorando a qualidade de vida da população.

Ao se definir periculosidade como a probabilidade de ocorrência de um incidente criminal, nota-se que existe a necessidade de criar um sistema inteligente capaz de medir os níveis de periculosidades em determinados locais e horários específicos, realizando uma predição através de dados históricos, cruzados com dados atuais, colhidos em tempo real por meio de registros de ocorrências e monitoramento das câmeras de segurança, para que possa antecipar ou estimar uma determinada situação. O intuito é gerar informações precisas para que as autoridades consigam agir, o quanto antes possível, para melhorar a segurança da população, sinalizando possíveis riscos, combatendo e mitigando os eventuais delitos que possam ocorrer nestas áreas.

Uma das abordagens mais modernas que vem sendo adotada nos últimos anos por diversas cidades é o reconhecimento facial e detecção de ações dos cidadãos, de forma automatizada, através da aplicação de algoritmos complexos de visão computacional nas inúmeras câmeras espalhadas pela cidade.

Estas ações obtêm informações em tempo real sobre a situação atual e permitem gerar alertas para que as forças de segurança possam atuar imediatamente, além de gerar subsídios para que as equipes de inteligência possam planejar ações eficientes de longo prazo minimizando o risco para as pessoas no futuro.

A iluminação das vias, praças, parques, quadras esportivas e ambientes de lazer em geral é outro fator importante para garantir a segurança pública. Locais bem iluminados são inoportunos para realização de ações criminais, por esse motivo, nota-se a necessidade de garantir um sistema de iluminação eficiente, realizando um monitoramento de luminosidade através de sensores

integrados com um sistema capaz de gerar informações atualizadas sobre a qualidade da iluminação das áreas com o maior índice de periculosidade.

Além do controle da iluminação, um fator que aumenta os índices de periculosidade é a ausência de funcionários responsáveis pela segurança em um determinado posto fixo, como, por exemplo, uma guarita. Manter os gestores informados sobre a existência de um posto desguarnecido auxilia no desenvolvimento de estratégias para definir qual será a melhor solução para resolver o problema.

Analisar a forma mais eficiente de integrar várias fontes de dados utilizando um sistema especialista capaz de captar informações sobre a qualidade da iluminação de regiões com níveis de periculosidade elevados, históricos de criminalidade e informações do trânsito em tempo real e transformá-las em informações pertinentes para a geração de uma ação preditiva é o desafio que esta pesquisa se propõe a resolver. Como resultado do processamento desses dados, é possível inferir um mapa de risco indicando o nível de periculosidade classificado em baixo, médio e alto.

A utilização de reconhecimento facial por câmeras, instaladas em pontos estratégicos, complementará o sistema especialista em sua missão de monitorar a cidade inteligente, tornando-a mais segura.

A meta deste trabalho é a análise da viabilidade da construção de um sistema especialista para o monitoramento por imagem e mapeamento geográfico dinâmico da periculosidade em uma cidade inteligente, que consiga representar, com significativa fidelidade, a probabilidade de ocorrência de incidentes dentro de um horizonte temporal predefinido, cruzando diferentes bases de informações, para inferir um mapa representativo do risco.

2 DEFINIÇÃO DO PROBLEMA

Uma cidade inteligente precisa ser segura para os seus cidadãos, e para alcançar este objetivo é necessário usar eficientemente os finitos, e algumas vezes até escassos, recursos disponíveis. Para que estas decisões de alocação de esforço sejam corretamente obtidas é recomendável utilizar um sistema de monitoramento muito preciso e ágil para a tomada de decisão em tempo real e que ao mesmo tempo possa gerar dados históricos confiáveis para a implementação de políticas públicas eficazes.

O objetivo deste trabalho é analisar a forma mais eficiente para construir um sistema computacional para monitorar a cidade inteligente e trabalhar em conjunto com a sociedade para mantê-la segura.

Para isto é preciso entender o contexto da segurança de uma cidade inteligente, todas as fontes de dados que possam e precisem ser monitoradas, quais os requisitos funcionais o sistema deve satisfazer, quais ações ele precisa tomar automaticamente, quais notificações precisa gerar para atuação humana de forma imediata.

Avaliar corretamente este contexto é o que vai garantir o seu bom funcionamento operacional e principalmente que os cidadãos se sintam seguros e bem atendidos em suas necessidades diárias.

Muitas técnicas vêm sendo empregadas, buscando compreender os motivos do crescimento da violência, as dimensões deste problema e identificar grupos e populações de maior risco.

O número de ocorrências e a evolução crescente dos homicídios no Brasil, representam, em última instância, indicadores ruins das condições de vida, dos padrões de relacionamento e das garantias de qualidade de vida.

Assim, ao investigar o problema da violência, confronta-se com a complexidade de composição, uma vez que, ao contrário de muitos outros problemas da área, a violência tem raízes em determinações múltiplas e inter-relacionadas, inerentes a diferentes disciplinas e setores da sociedade.

Atualmente os dados referentes à criminalidade são normalmente agrupados um a um, a partir de diferentes e pequenas fontes, formando uma “colcha de retalhos”, medindo os tipos de crimes cometidos nas grandes cidades.

Esse cenário sinaliza uma dificuldade do planejamento efetivo de políticas públicas que possam combater a violência e a criminalidade, prevenindo tais delitos.

A associação entre processos de rápido crescimento urbano e o aumento nas taxas de violência tem sido o grande pilar no qual se apoiam estudos sociológicos sobre a criminalidade na cidade.

De acordo com esses estudos, processos rápidos de industrialização e urbanização provocam intensos movimentos migratórios, concentrando massas de pessoas isoladas nas periferias dos grandes centros urbanos, sob condições de extrema pobreza e desorganização social e exposta a novos comportamentos e aspirações mais elevados, inconsistentes, com possibilidades disponíveis. As rápidas mudanças sociais são o ambiente propício para a expansão da violência e criminalidade nas grandes cidades.

As ocorrências criminais possuem características bem definidas, como tipo, localização e horário, que precisam ser compreendidas e analisadas para definir as políticas públicas e enfrentar o problema da violência na sociedade.

A segurança é um dos assuntos mais relevantes da vida humana. Segundo a Pirâmide de Maslow (MASLOW, 1943), é possível constatar que garantir a integridade física e patrimonial de todos os cidadãos é de suma importância para que estes possam ter uma boa qualidade de vida, ocupando o segundo nível de necessidade, logo acima da sobrevivência.

A percepção de segurança é um conceito abstrato que representa a sensação de proteção, uma representação do mundo, se a situação que se apresenta naquele momento possui ou não uma probabilidade maior de ocorrer um incidente de segurança.

Algumas pessoas podem se sentir inseguras no mesmo local onde outras não se sintam desta mesma forma, além do fato de que um crime possa ocorrer em localidades consideradas seguras historicamente.

Atualmente a maior quantidade de crimes ocorre nas cidades. Observando-se que em 1800 somente 3% da população mundial vivia em cidades, já em 2010 este percentual ultrapassou 50% (INDEX MUNDI, 2012) e é estimado que atinja 70% em 2050 (WILSON, 2012), verifica-se que este problema tem se tornado cada vez mais complexo e difícil de ser administrado pelos

responsáveis pela segurança pública, principalmente das grandes metrópoles, e o Brasil possui algumas das cidades mais violentas do mundo (UOL, 2014).

É impressionante notar que as cidades mais populosas e também mais importantes da atualidade foram projetadas e funcionam estruturalmente quase da mesma forma há mais de 200 anos (MIT, 2014).

Dividindo a cidade em infraestrutura, serviços e pessoas, na imensa maioria delas o número de pessoas cresce mais rapidamente do que os outros dois componentes conseguem acompanhar, criando-se assim os gargalos.

Para que se possa transformar a cidade em um lugar melhor para todos é necessário torná-la mais inteligente, ou seja, que ela possa ser capaz de prestar um serviço melhor para as pessoas, utilizando mais eficientemente a infraestrutura instalada (CHOURABI, 2012) e detectando o mais precocemente possível a necessidade de novos investimentos.

2.1 IMPORTÂNCIA E COMPLEXIDADE DOS DADOS

É necessário e oportuno construir uma estrutura computacional capaz de receber e tratar o volume de dados que são disponibilizados extraindo informações úteis dele, em tempo suficiente para serem usadas pelos agentes públicos e privados na promoção de um serviço de melhor qualidade para todos os habitantes. Isto significa organizar melhor as ações preventivas ou mesmo otimizar com inteligência o consumo de recursos limitados e muitas vezes escassos, como equipamentos e pessoas.

A eficiência deve ser a meta principal do gestor de uma cidade inteligente e para alcançá-la, é preciso tomar decisões baseadas em dados, modelos matemáticos e algoritmos confiáveis, e que gerem informações relevantes.

Tornar segura uma cidade, convergindo-a para uma Cidade Inteligente, é um desafio grandioso e complexo. A consolidação das informações fragmentadas, provenientes de diferentes fontes dos dados, é o primeiro passo para tomar as melhores decisões de planejamento e também responder com qualidade aos eventos que se apresentam.

Outro desafio igualmente importante é garantir que os dados sejam confiáveis e sempre atualizados, pois eles sempre serão o ponto de partida para

todas as análises subsequentes, sem estas garantias quaisquer resultados apresentados não serão corretos.

Os dados necessários para subsidiar esta inteligência podem ser classificados em três categorias:

1) Históricos: acontecimentos prévios que ajudam a formar a base inicial de conhecimento;

2) Gerados pelas pessoas: podem ser feitos diretamente e em tempo real, como chamados abertos por telefones, websites e aplicativos mobile, ou indiretamente, como postagens em redes sociais de acontecimentos (FERRAZ, 2013), sugestões e reclamações;

3) Gerados por equipamentos eletrônicos: informações adquiridas de sensores e câmeras (PERERA et al., 2013; JUNG, 2013; CALAVIA, 2012).

O desafio em receber, analisar e armazenar vídeos vindos de milhares de câmeras simultaneamente é imenso, pois os vídeos costumam ter tamanhos grandes (em bytes) e há a necessidade de câmeras de alta resolução para utilização no reconhecimento facial.

O número de dados gerados na internet vem crescendo exponencialmente com o passar dos anos, segundo Bernard Marr (2015), escritor e consultor corporativo especializado em Big Data e desempenho empresarial, a quantidade de dados armazenados atualmente é de aproximadamente 4,4 zettabytes (ZiB) e, em até 5 anos, esse volume deve passar para cerca de 44 zettabytes (ZiB) ou 44 trilhões de gigabytes (1 ZiB = 10^{21} bytes).

Tudo indica que até 2020 cerca de 1,7 megabyte de novas informações serão criadas por segundo para cada uma das pessoas no planeta (MARR, 2015).

2.2 USO DE DADOS PÚBLICOS

Para um sistema de monitoramento ser eficiente ele precisa extrair informações de fontes de dados externos, em grande parte imagens de

monitoramento de ruas e ambientes fechados de grande circulação pública, como metros, ônibus, estádios, hospitais, etc.

Na maioria dos países existem legislações que regulam o uso e divulgação destas informações contidas nas imagens dos vídeos, em alguns deles existem instruções mais ou menos liberais sobre quem pode ter acesso e quais são as aplicações possíveis para elas.

Existe uma grande discussão sobre a preocupação com a privacidade e principalmente o limite do Estado sobre seus cidadãos que deve sempre ser levada em consideração quando se trata de vigilância pública, em que o grande desafio é equilibrar a necessidade legítima por segurança, resguardando o direto à privacidade e confidencialidade sobre a vida privada.

As entidades públicas podem tornar o sistema ainda mais eficiente se forem capazes de se conectar a fontes extras de captura de imagens, tais como câmeras de monitoramento de calçada de lojas e condomínios, ampliando assim a cobertura de vigilância, podendo monitorar um espaço maior, permitindo se antever a situações de risco.

3 PESQUISA BIBLIOGRÁFICA

A segurança é um conceito abstrato, ainda assim existem diversos trabalhos (HART; ZANDBERGEN, 2012; JUNG, 2013) que buscam mapear com boa precisão as áreas com maior risco, permitindo assim que os responsáveis possam responder adequadamente a esta situação.

Verifica-se que existem duas características pouco exploradas nestes trabalhos e que se procura avançar aqui:

1) Dependência temporal no perfil dos crimes: o tipo, alvo, criminoso, vítimas e localização se modificam com o horário do dia e dias da semana;

2) Influência de fatores externos na oportunidade: modificações na probabilidade de ocorrência de crimes com fatores externos, como, por exemplo, falha na iluminação pública ou congestionamento no trânsito.

Busca-se analisar a melhor forma para se construir um sistema especialista de mapeamento da segurança levando em consideração esses fatores, o que tornará o processo de previsão mais aderente à realidade, permitindo um aumento da sua eficiência.

Foram feitas também revisões bibliográficas sobre estudos realizados nas áreas de iluminação, segurança e análises criminais para geração de conhecimento com ênfase em prevenção.

Analisou-se artigos sobre visão computacional, principalmente aqueles voltados para o reconhecimento facial e objetos, seus diferentes algoritmos, vantagens e desvantagens para o uso nas situações mais prováveis no monitoramento de cidades.

Este sistema deve utilizar modelagens de dados especificas para suportar grandes volumes de informações, conceito chamado de Big Data, tema este que foi igualmente coberto por artigos com enfoque mais conceitual.

3.1 LIBERALIDADE TECNOLÓGICA NA CHINA

A China em 2016 decidiu que Inteligência Artificial seria uma das suas áreas prioritárias para investimento governamental, seja diretamente ou através das suas maiores empresas de tecnologia tais como Baidu, Alibaba e Tecent (JIA, 2018), desde então está na vanguarda do uso desta tecnologia e provavelmente possui o programa de vigilância de segurança por câmeras do mundo mais avançado da atualidade.

O país possui 170 milhões de câmeras funcionando ininterruptamente e até 2023 a previsão é que sejam instaladas mais 400 milhões.

Como demonstração da eficiência do sistema a foto de um repórter da BBC foi cadastrada e após somente 7 minutos ele foi abordado por policiais na rua (LIU, 2017).

Na China já se usa a face como senha do banco e em diversos outros serviços pessoais, como pagamento de transporte público e lojas e liberação de acessos em locais restritos.

O país ainda tem um projeto ambicioso de transformar este processo em um sistema de vigilância ainda mais extenso, com a análise do comportamento das pessoas em espaços públicos, o que provocará pontuações positivas e negativas para bons e maus comportamentos.

Atualmente, caso uma câmera reconheça o cometimento de uma infração, como atravessar a rua fora da faixa de pedestre ou jogar lixo no chão, automaticamente são registradas multas financeiras subtraindo valores diretamente na carteira digital do infrator em aplicativos como WeChat e AliPay (THE ECONOMIST, 2018).

3.2 RESTRIÇÃO DE USO DE RECONHECIMENTO FACIAL EM SÃO FRANCISCO

São Francisco é um exemplo de cidade onde recentemente foi proibido o uso de Reconhecimento Facial por órgãos públicos para monitorar seus cidadãos.

Levou-se em consideração principalmente os seguintes fatores:

1) Privacidade: as pessoas devem poder manter seus atos em locais públicos sigilosos, tais como aquilo que eles fazem, com quem se encontram, quais horários, de que forma se locomovem, etc.;

2) Preconceito: alguns estudos comprovam que existem imprecisões maiores no reconhecimento facial de mulheres negras em comparação com homens brancos e desta forma pode levar a erros de reconhecimento e uma imputação de crime ou atitude;

3) Imprecisão: demonstrou-se que alguns sistemas comercializados por grandes empresas possuem imprecisões no reconhecimento de pessoas como suspeitos, inclusive identificando pessoas idôneas (como congressistas americanos) como criminosos procurados (SINGER, 2018).

Em razão desta restrição não é possível utilizar o reconhecimento facial para monitoramento público de segurança nesta cidade atualmente.

É importante que o avanço tecnológico, ético e regulatório avancem juntos e de forma equilibrada para superar estes aspectos relevantes para trazer a tranquilidade necessária para que possa ser utilizada de forma justa e eficiente.

3.3 CIDADES INTELIGENTES

O grande desafio tanto para a segurança pública quanto para todos os governos é o aumento da complexidade para monitorar eficientemente seus habitantes nas cidades.

A tecnologia de reconhecimento facial tem a capacidade de vir a ser uma grande colaboradora na identificação de suspeitos sinalizando às autoridades para uma rápida interceptação desses indivíduos.

Devido ao aumento exponencial de câmeras nas principais metrópoles do mundo, torna-se praticamente impossível que a monitorização eficaz e ininterrupta seja feita por seres humanos.

Com o uso de softwares projetados com modernos algoritmos de Visão Computacional, uma das subáreas da Inteligência Artificial, a investigação de grandes quantidades de imagens em vídeos e fotos é possível bem como a busca

por padrões previamente treinados, como rostos, placas, objetos e automóveis, gerando dessa forma alertas somente com uma probabilidade muito alta de identificação.

Os seres humanos podem fazer o reconhecimento facial de maneira bem precisa, mas existe uma limitação na capacidade em lidar com grandes quantidades de imagens, além de alguns elementos que possam ser utilizados de maneira propositada ou acidental, com o objetivo de gerar confusão ou para disfarces, tais como modificação e ocultação do rosto, e também o fato de que os suspeitos possam ter as imagens antigas no banco de dados.

No entanto, quando empregam-se técnicas computacionais para treinamento dos algoritmos, mesmo com tais aspectos de uso de disfarces ou mudanças faciais mantêm-se ser precisas, ainda que lidando com imensas quantidades de informações simultaneamente, pois é possível a utilização de técnicas de buscas por características parcialmente visíveis segmentando as imagens ou mesmo a reconstrução das partes faltantes utilizando interpolação, em alguns casos somente são necessárias poucas características para executar a correta diferenciação para classificação (WRIGHT, 2008).

No processo chamado de Hyper Vigilância, as pessoas são averiguadas quanto a com quem se encontraram, onde estiveram e em quais horários. Entretanto, são muitas as preocupações e opiniões contrárias de diversas entidades preocupadas com a quebra da liberdade individual devido à falta de privacidade das informações e o direito do Estado na monitorização constante dos cidadãos.

3.3.1 Sistema Especialista

A construção de um Sistema Especialista justifica-se por sua capacidade de contribuição na geração de resultados úteis para seus usuários, que apoiam de modo eficaz a tomada de decisão mais acertada, em menor tempo e custo.

Um Sistema Especialista é capaz de analisar uma grande quantidade de informações com ferramentas matemáticas para buscar correlações entre as variáveis de entrada e com isto inferir previsões em velocidades significativamente superiores à capacidade de um ser humano.

Além disso, consegue-se desta forma tornar o processo decisório mais científico e menos baseado em opiniões pessoais, o que ao longo do tempo, com os devidos aprimoramentos e aprendizados, levarão a resultados mais eficientes e duradouros, ou seja, que consigam manter a criminalidade a níveis menores historicamente em linha com os padrões internacionais.

Outra característica relevante é a redução do efeito da corrupção, pois é significativamente mais complicado distorcer as indicações geradas pelo sistema especialista do que por outros tipos de planejamento feitos manualmente ou mesmo por sistemas sem nenhuma rastreabilidade e possibilidade de auditorias confiáveis.

A pergunta que se pretende responder nesse trabalho é como se deve construir um sistema especialista que possa auxiliar os gestores de segurança gerando informações precisas e confiáveis, dando suporte para que eles possam realizar as tomadas de decisões preditivas, de forma ágil e eficiente, com o propósito de atender às expectativas da população referentes à segurança pública.

A inovação proposta nesta pesquisa é o desenvolvimento de um sistema preditivo, que realize a análise das causas-raiz dos problemas, e sinalize com antecedência as áreas que estão mais propensas a ocorrências de incidentes criminais, considerando além do histórico, também os fatores de horário, luminosidade e trânsito. Atualmente a polícia militar de São Paulo utiliza-se de sistemas para a análise de incidentes, que geram informações dos índices de criminalidade através dos dados históricos, ou seja, dos fatos ocorridos.

As análises de prevenção são realizadas pelos gestores através das suas experiências pessoais prévias, em conjunto com as informações das áreas que possuem os maiores índices de criminalidade que são geradas por esses sistemas de monitoramento. O Detecta, utilizado pela Polícia Militar do estado de São Paulo, por exemplo, é um sistema de monitoramento em tempo real, realizado através da integração de banco de dados e câmeras de diferentes instituições para monitorar áreas específicas, veículos e suspeitos auxiliando os policiais militares e civis no combate da violência.

De forma semelhante às ferramentas existentes no mercado, o sistema especialista deverá ser capaz de realizar análises de periculosidade de determinadas áreas, utilizando-se de dados históricos. O que faz o sistema

especialista ser um método inovador é o acréscimo de três fatores para a realização destas análises, que são os fatores de horário, luminosidade e trânsito. Com isso é possível gerar alertas, mapas e relatórios com informações preditivas das áreas mais propensas a ações criminais, auxiliando os gestores a agirem antes que os incidentes ocorram, ou seja, prover informações para a prevenção de ações criminais.

3.4 VISÃO COMPUTACIONAL

A visão computacional é a subárea da Inteligência Artificial que estuda e desenvolve os algoritmos responsáveis por extrair informações de imagens, sejam elas estáticas (fotografias) ou dinâmicas (vídeo).

Esta atividade é muito importante, pois permite monitorar, analisar, medir, estimar, contar diversas situações do mundo real em que seria necessário um profissional treinado para executar a tarefa.

Com o aprimoramento nos últimos anos dos algoritmos, novas descobertas de técnicas complexas e a possibilidade de utilização de hardwares cada vez mais poderosos, a visão computacional está obtendo resultados superiores aos melhores especialistas humanos naquela tarefa em diversas situações.

Sejam tarefas trabalhosas, como, por exemplo, contar milhares de pessoas em uma imagem de uma multidão, em que o tempo de resposta é muito menor ou a complexa e altamente especializada tarefa de identificação de um tumor em uma imagem de ressonância magnética, que em alguns casos já superam a precisão dos médicos.

Em grande parte a visão computacional consiste em construir algoritmos altamente especializados na identificação de padrões complexos em uma imagem.

Uma das aplicação mais pesquisadas atualmente da visão computacional é como utilizá-la para gerar interação inteligente diretamente com o ambiente, permitindo que robôs e carros autônomos consigam se movimentar e tomar as decisões corretamente reagindo de maneira instantânea às mudanças em seu campo de visão.

3.4.1 Finalidade do Reconhecimento Facial

A principal função dos métodos de reconhecimento facial em cidades inteligentes é a investigação de criminosos procurados pela justiça.

Outra atribuição social importante é a procura por pessoas desaparecidas, principalmente idosos e crianças, que podem não conseguir voltar ou ainda se perder por diversas razões, como sequestro, desconhecimento do endereço pessoal, amnésia repentina por desmaios, acidentes ou ocasionada por doenças como Alzheimer.

As pessoas desaparecidas por um longo período têm seus rostos modificados, o que pode vir a ser uma dificuldade no reconhecimento por um assistente social, como corte de cabelos, envelhecimento facial, rugas, crescimento (no caso de crianças), mudanças estéticas e corporais.

Um acidente sofrido pode gerar inconsciências e por este motivo estas pessoas não têm a capacidade de passar dados pessoais.

Para os seres humanos, o reconhecimento de rostos envelhecidos ou com mudanças estéticas é muito difícil, e mesmo para os computadores, devido à quantidade e intensidade das mudanças na pele em alguns dos elementos do rosto, executar esta tarefa é algo bastante complexo. Existem algoritmos específicos que combinam tanto a análise de características quanto as distâncias entre os elementos para maximizar a possibilidade de encontrar a pessoa correta, mesmo com os efeitos do envelhecimento (LI, 2018).

Uma forma de aumentar significativamente as chances de encontrar alguém desaparecido num tempo reduzido é o cadastramento de tais pessoas nos serviços de buscas de pessoas desaparecidas. As câmeras posicionadas em locais públicos monitoram de forma constante a cidade e podem ser acionadas pelos serviços de buscas a fim de procurar as pessoas desaparecidas cadastradas. É possível também a integração com locais privados especiais para onde os desaparecidos podem ter sido levados após alguma ocorrência, tais como hospitais e abrigos.

3.4.2 Detecção Facial

O processo chamado de detecção facial é identificar se numa imagem genérica existe ou não um ou mais rostos humanos.

Para a detecção de objetos, em geral os sistemas pesquisam obter a fronteira entre eles, normalmente definidos por uma alteração repentina de contraste em uma parte da imagem, mudança de forma ou então um modo característico daquele objeto que está sendo buscado.

Quando um algoritmo de detecção é planejado para identificar rostos humanos, cujas características são de certa forma parecidos, ele pode ser desenvolvido para distinguir formas relevantes, tais como uma boca, duas narinas em um nariz e dois olhos.

3.4.3 Reconhecimento Facial

O reconhecimento facial é uma função bastante complexa, que demanda a utilização de algoritmos que possam retirar dados sobre os rostos humanos, tornando-os identificadores exatos e pouco mutáveis no decorrer do tempo.

O método de reconhecimento facial opera com as seguintes etapas:

– Seleção e planejamento do algoritmo de detecção facial: definição do algoritmo responsável pela verificação da existência de uma face humana em determinada imagem, seleção desta área da imagem e envio para o algoritmo de reconhecimento facial. O algoritmo analisado será o Viola-Jones;

– Definição do planejamento do algoritmo de reconhecimento facial: são diversas as formas de reconhecimento de rostos humanos, sendo aqui apresentadas três possíveis estratégias para execução desta tarefa: análise de características físicas, Eigenfaces e Fisherfaces;

– Capacitação do algoritmo de reconhecimento: feita a escolha, é preciso importar para a base de conhecimento do algoritmo todos os rostos aos quais exista o interesse em identificar nas câmeras.

– Encaminhamento das imagens para análise pelo sistema: interligação das câmeras responsáveis pela captura das imagens com o algoritmo de detecção facial;

– Criação de alertas para os responsáveis: no caso de que alguma face previamente cadastrada seja identificada, um alerta imediato deve ser gerado com a identificação e localização do indivíduo.

Algumas técnicas para executar esta tarefa foram elaboradas, das quais duas se destacam:

– Pesquisa de aspectos faciais: constatar e verificar o posicionamento das marcas expressivas do rosto, tais como olhos, boca, nariz e com estes dados estabelecer uma identificação numérica composta desta face;

– Semelhança com reproduções faciais convencionais: imagens que possam identificar partes do rosto de uma base de dados são geradas e cada pessoa é representada de acordo com um arranjo sequencial da sua semelhança com cada um destes itens determinados antecipadamente.

Apesar destas técnicas terem seus benefícios e inconveniências, atualmente os algoritmos rastreadores de semelhanças com representações faciais padronizadas são os mais utilizados, devido à sua precisão e rapidez no desempenho.

3.4.4 Investigação de Características

O início do desenvolvimento dos estudos na área de reconhecimento facial deu-se na década de 1960, com os pesquisadores Woody Bledsoe, Helen Chan Wolf e Charles Bisson (ALBAKRI; ALMAMORY; ALFARTOSY, 2018). Entretanto, há pouca publicação dos dados em razão dos estudos terem sido financiados por uma agência governamental de inteligência.

Iniciava-se o reconhecimento facial por características por meio da análise de dados relevantes, tais como os olhos, nariz e boca; o mapeamento inicial era realizado de forma manual.

Hoje em dia, filtros são aplicados nas imagens recebidas, retirando todos os dados marcantes para a identificação reforçando-se os pontos buscados, assim, uma filtragem mais eficiente da face é obtida.

Depois disso, os pontos relevantes são marcados e mapeados, como:

– Olhos: centro da íris, canto dos olhos, diâmetro da pupila;

– Nariz: tamanho, posição das narinas;

– Boca: posição dos cantos da boca, largura e comprimento dos lábios;

– Rosto: contorno e formato das extremidades, como testa e queixo.

O uso de algoritmos que identifiquem objetos pelas extremidades e semelhanças com figuras conhecidas é realizado a fim de se conseguir reconhecimento dos pontos importantes do rosto.

Após o mapeamento dos pontos relevantes, a distância entre eles é calculada, agrupando as medidas de distâncias relativas e absolutas, bem como o ângulo de inclinação entre as retas que os interligam, criando assim uma identificação única da face do indivíduo. Este dado é registrado na base de dados em formato de vetor para futura consulta.

No recebimento de uma nova imagem de face, executa-se o processo de identificação dos pontos relevantes e o cálculo das medidas de distâncias, o resultado é então comparado com os dados armazenados no banco de dados produzido, com o objetivo de encontrar a melhor semelhança, calculando a distância euclidiana para os já anteriormente armazenados.

Uma vez averiguada uma distância menor do que o valor máximo de erro permitido, a face identificada é reconhecida como igual àquela armazenada na base de dados.

No entanto, para o amplo uso destes algoritmos, muitos desafios são levantados, uma vez que o meio para definir todos os pontos semelhantes de um

determinado rosto tem um custo de processamento bastante elevado computacionalmente.

É necessário também guardar uma grande quantidade de dados por face, em virtude da extensão que o vetor terá pela combinação de distâncias e ângulos entre os pontos e o cálculo da distância euclidiana para comparação, que também será intensivo.

3.4.5 Algoritmo Viola-Jones

Este algoritmo recebeu este nome porque foi proposto pelos pesquisadores Viola e Jones (2001), cuja intenção era construir um software que fosse eficiente e veloz na detecção de objetos em tempo real, em particular no reconhecimento facial.

Para a identificação dos rostos há uma sequência de passos a ser executada, tais quais:

– Características Haar: busca-se na imagem do rosto determinadas características, como a região dos olhos que é em geral mais escura do que as bochechas e a região do nariz que é mais clara do que os olhos;

– Transformação em uma imagem completa: uma representação matemática da somatória de todos os valores anteriores agiliza as operações para a identificação das diferenças significativas de contrastes entre as áreas;

– Algoritmo AdaBoost: este algoritmo utilizado em machine learning permite encadear diversas árvores de decisão simples, que separadamente seriam categorizados como classificadores fracos e os combinar ordenadamente de maneira eficaz, complementando com um algoritmo de reforço de treinamento representado na forma de pesos de votação. Assim consegue-se obter um classificador robusto, complexo e bastante preciso, mesmo partindo-se de uma estrutura inicial simples (FREUND; SCHAPIRE,1996).

– Classificadores em Cascata: inicialmente são utilizados os mais simples com respostas mais amplas para posteriormente serem adicionados os mais complexos e precisos somente em áreas que tenham alta probabilidade de encontrar rostos. Quando uma imagem é descartada em um filtro ela não precisa seguir sendo avaliada pelos demais.

Com o uso deste método há a possibilidade de identificação de mais de um rosto em uma imagem com um retorno rápido o suficiente para processar em tempo real em computadores comuns, sendo possível melhorar significativamente processando as informações com o uso do GPU (Graphics Processing Unit) ao invés de fazê-lo da forma tradicional utilizando a CPU (Central Processing Unit), vide item 4.6 para processar este algoritmo (HEFENBROCK et al., 2010).

Depois da definição da área do rosto uma chamada subsequente para o algoritmo de reconhecimento é feita para a identificação em sua base de dados.

3.4.6 PCA (Principal Component Analysis)

O PCA (Principal Component Analysis) é uma transformação matemática ortogonal inventada em 1901 pelo estatístico inglês Karl Pearson, que procura identificar os componentes principais de uma amostra, representando de forma mais simplificada toda a população de amostras.

Utiliza como critério para escolher os componentes principais aqueles que possuírem a maior variância possível.

A utilização deste algoritmo é importante para permitir uma redução significativa da complexidade de quando são utilizados autovalores ao mesmo tempo que procura minimizar os efeitos desta simplificação, identificando os elementos mais representativos para maximizar o resultado mesmo com uma quantidade menor de componentes.

3.4.7 LDA (Linear Discriminant Analysis)

O LDA (Linear Discriminant Analysis) é uma análise discriminante desenvolvida por Sir Ronald Aylmer Fisher em 1936, também um estatístico inglês.

Esta técnica encontra as características que melhor consigam separar as amostras em classes diferentes, na maioria das vezes é utilizada de forma supervisionada para ser possível atribuir as nomenclaturas para cada uma das classes identificadas.

A principal vantagem quando este algoritmo é utilizado é a identificação de uma descrição de classes mais robustas entre si, pois mesmo que exista um ruído ainda assim a outra classe estará suficientemente distante e a probabilidade de uma classificação errada é menor.

3.4.8 Eigenfaces

Neste sistema cada rosto é representado por um arranjo linear de diversos componentes, sendo assim um processo mais eficiente do que a classificação baseada em características (TURK; PENTLAND, 1991).

A palavra alemã *eigen* significa “próprio” e é usado referindo-se aos autovetores e autovalores calculados em álgebra linear.

As Eigenfaces podem descrever as características principais dos rostos armazenados em um determinado banco de dados, e estes componentes são os autovetores (ou eigenvetores).

Com o PCA (Principal Component Analysis), vide item 3.4.6, é possível definir quais elementos melhor caracterizam o conjunto de rostos armazenados no banco de dados, rastreando aqueles que tenham uma variação maior em relação à média e sejam ortogonais entre si, diminuindo dessa forma o uso de muitas Eigenfaces que configurem de maneira precisa um rosto real.

O método de codificação das faces utilizando Eigenfaces é feito da seguinte forma:

– Converter para um vetor: torna uma imagem na forma de uma matriz em pixels em um vetor;

– Mudança do referencial: retira a média deste vetor diminuindo de cada rosto como sendo somente o valor de diferença entre a média e a sua reprodução original;

– Cálculo de todos os prováveis Eigenvetores e Eigenvalores da matriz de covariância;

– Definição dos melhores Eigenvetores para representação: uso do algoritmo PCA para a organização dos Eigenvetores que melhor representam a amostra de dados.

Assim sendo, a condição de possuir uma grande quantidade de imagens que representem as características principais dos rostos diminui, formando um subconjunto eficaz de componentes.

Sendo possível encontrar em todos os componentes viáveis àqueles que são mais aptos na representação, pode-se ter agilidade e precisão com uma pequena quantidade nas figuras selecionadas.

Com um armazenamento de somente 10 ou 20 bytes para codificar 10 ou 20 Eigenfaces, respectivamente, é possível ter uma representação muito eficiente e fácil de rastreio para comparação.

Buscar um rosto em um banco de dados organizado desta forma é muito eficiente, mas é preciso que as imagens salvas e aquelas que estão sendo utilizadas para fazer a consulta tenham sido registradas em locais controlados, especialmente na questão da luminosidade e do ângulo.

Essa técnica de reconhecimento facial demonstrou ter dificuldade no procedimento quando as características externas não são ideais, como a luminosidade e no caso de objetos que cubram parcialmente o rosto, como o uso de boné e capuz ou óculos (BELHUMEUR; HESPANHA; KRIEGMAN, 1997).

3.4.9 Fisherfaces

As interferências externas ocorrem de maneira frequente em ambientes não controlados das cidades, portanto, foi preciso encontrar um conjunto de características que sofresse menos com estas situações.

Para tanto, a técnica LDA (Linear Discriminant Analysis), vide item 3.4.7, é utilizada, ao invés de PCA (Principal Component Analysis), para a busca de características relevantes e redução da complexidade.

Este método matemático para compor a combinação linear recebeu este nome devido ao seu desenvolvimento por Sir Ronald Fisher em 1936.

Esta técnica rastreia as amostras que representam da melhor forma um determinado cluster, assim discrimina melhor a representação dos elementos separando os diversos indivíduos eficientemente (BISSI, 2018).

Ao contrário da técnica Eigenfaces, as Fisherfaces não tentam encontrar os rostos que melhor representam a média armazenada na base de dados, mas as características principais de tais rostos.

De acordo com Hegde, Preetha e Bhagwat (2018), o uso do método Fisherfaces é mais eficiente para o processamento de imagens faciais capturadas em situações reais.

3.4.10 Rostos identificados com qualidade

Um importante aspecto do sistema de reconhecimento facial é a visualização completa do rosto a ser analisado.

Este ponto é realmente relevante, pois diversas características precisam ser extraídas da face para construir o vetor de característica do rosto visualizado naquela imagem e assim poder comparar com aqueles demais armazenados previamente no banco de dados.

Porém, quando as imagens são capturadas por sistemas reais utilizados em locais movimentados é muito provável que diversas pessoas tenham suas imagens capturadas em fotografias (ou um frame isolado de um vídeo contínuo) em ângulos desfavoráveis, com os seus rostos parcialmente obscurecidos.

É preciso levar em consideração também o dinamismo do ambiente, visto que uma determinada rua que esteja sendo filmada não se mantém nas mesmas

condições continuamente, existem diferenças de iluminação natural e artificial, sombras de objetos e das pessoas sendo projetadas umas nas outras, eventos como chuva, garoa, neblina que modificam a nitidez das imagens temporariamente.

Existem alguns fatores relevantes que levam a estas situações, tais quais os definidos a seguir.

3.4.10.1 Pose

A pose é a forma que é qualificada a posição horizontal da face, ou seja, ela pode se apresentar nas seguintes formas:

– Frontal: visualização completa do rosto, inclusive sendo possível identificar as duas orelhas do cidadão;

– Parcialmente rotacionado: visualização parcial do rosto, sendo possível identificar um lado completamente e parte do outro lado, principalmente os dois olhos;

– Lateral: visualização somente de um dos lados do rosto, não sendo possível enxergar a segunda metade da face;

– Costas: não é possível enxergar nenhuma característica frontal do rosto.

A maioria dos algoritmos consegue extrair informações precisas somente obtendo uma Pose Frontal, pois é necessário extrair diversos pontos relevantes do rosto para então iniciar a análise comparativa entre aqueles que já estejam armazenados no banco de dados.

Entretanto, diversas situações geram imagens com poses não ideais para finalidade de reconhecimento facial, como, por exemplo, uma má escolha do local de fixação, deslocamento acidental da câmera (colisão com objeto, vento, chuva, etc.) ou mesmo situações em que a câmera foi colocada em uma posição onde consegue capturar frontalmente uma boa parte do fluxo de pessoas, porém

aquelas que passam nas laterais têm a sua pose parcialmente rotacionada, por exemplo, uma entrada ou saída de uma estação de metrô de grande movimento.

Nestes casos, é importante que sejam utilizados três tipos de situações de contorno para maximizar os resultados obtidos:

1) Ajustar o algoritmo de detecção facial (por exemplo, Viola Jones) para que ele reconheça aquele objeto como sendo uma face, mesmo que parcialmente obscurecida e a envie para um algoritmo de correção da pose;

2) Algoritmo de espelhamento de imagem: é possível utilizar técnicas para reconstruir o rosto parcialmente ocultado, usando o espelhamento da forma, cores e tamanhos relativos obtidos na parte do rosto que esteja visível. Esta técnica leva em consideração que na imensa maioria dos casos, os dois lados do rosto são simétricos, salvo por situações de rara ocorrência como cicatrizes, modificações naturais na pele (pintas, manchas, etc.) ou modificações artificiais como tatuagens. Constrói-se uma versão 3D da face e depois planifica-se em 2D para a aplicação do algoritmo de reconhecimento;

3) Algoritmos de complemento de imagem: é possível gerar algumas combinações de imagens com informações faltantes para encontrar prováveis pessoas, como, por exemplo, sobrepondo uma imagem-padrão quando a foto encaminhada está com os olhos fechados, com a língua de fora, utilizando um óculos escuros.

3.4.10.2 Inclinação da cabeça

Outra forma de ocultação parcial da face é a inclinação da cabeça. Neste caso, diferentemente da pose, a mudança é sobre a inclinação vertical do rosto e poderá se dar da seguinte forma:

– Frontal: visualização completa do rosto, inclusive a testa e o queixo estando plenamente visíveis;

– Inclinado parcialmente para baixo: é possível enxergar a testa, os olhos e o nariz;

– Inclinado parcialmente para cima: é possível enxergar o queixo, a boca e o nariz;

– Totalmente inclinado para baixo: visualiza-se somente a cabeça, não é possível observar nenhuma parte do rosto;

– Totalmente inclinado para cima: visualiza-se somente o pescoço, não é possível observar nenhuma parte do rosto.

Esta situação é mais complexa de ser tratada do que aquela da pose, pois normalmente na situação de ser preciso reconstruir uma imagem baseada em uma pose desfavorável é possível aproveitar a característica de simetria para reconstruir as partes faltantes espelhando o lado que se conseguiu obter na imagem original.

Para se tentar otimizar nesta situação é necessário aprimoramento em dois aspectos:

1) Novamente ajustar o algoritmo de detecção facial para que seja classificado como um rosto, mesmo que falte alguma característica obscurecida e a encaminhe para o algoritmo de correção da inclinação;

2) Algoritmos de complemento de imagem: neste caso a melhor alternativa é reconstruir a imagem do rosto buscando remontar mediante um mosaico de imagens obtivas em fotografias ou frames anteriores.

3.4.10.3 Sombra

As câmeras espalhadas por uma cidade estão inseridas em locais com grande variação de luminosidade ao longo do dia.

A luminosidade costuma variar de forma muito intensa ao longo do dia, por diversas características:

1) Horário: manhãs, tardes e noites costumam ter claridades muito diferentes devido à exposição solar e lunar;

2) Iluminação externa: pode afetar a capacidade de contraste da câmera se ela for muito fraca, não permitindo a captura de uma imagem nítida ou, se for muito forte, por ofuscamento da câmera;

3) Época do ano: no verão a luminosidade é muito maior do que no inverno, mesmo durante o dia;

4) Chuva: durante a chuva a capacidade de observação de uma câmera de um objeto a distância diminui consideravelmente;

5) Anteparo externo: um objeto que seja posicionado entre a fonte de luz e a face a ser reconhecida pode gerar uma sombra que reduza a capacidade de análise, como, por exemplo, um toldo ou mesmo um simples guarda-chuvas.

6) Ofuscamento por fonte de luz: um feixe de luz pode ser direcionado frontalmente para a câmera, impedindo que ela consiga visualizar os objetos corretamente. Este efeito pode acontecer temporariamente, como, por exemplo, um farol alto de um carro ou continuamente em razão de uma lâmpada instalada muito próxima à câmera.

Existem algoritmos que conseguem melhorar significativamente a qualidade de uma imagem obtida sob condições de baixa luminosidade, aplicando filtros matemáticos para extrair eficientemente as características de contorno do rosto, pontos de contraste, minimizando ruídos gerados pelas sombras nestes objetos.

3.4.11 Detecção de Objetos

Existem algoritmos especializados na análise de objetos em imagens que fazem o reconhecimento devido às suas características previamente selecionadas.

Com este método é possível detectar objetos supostamente perigosos, tais como:

– Armas: reconhecer alguma pessoa portando uma arma, de fogo ou branca, e gerar um alerta preventivo;

– Rosto coberto: quando uma pessoa estiver com o rosto coberto por uma máscara, por exemplo, justifica-se criar um pedido de análise;

– Explosivos: identificação de objetos possíveis de colocar em risco um grande número de pessoas ou um patrimônio público;

– Veículos em locais restritos: alguns ataques contra pessoas já foram feitos com veículos.

Outro assunto a ser explorado, como exemplo, seria um assalto a banco ou a um estabelecimento comercial, em que a partir de uma detecção de emergência, um sistema poderia seguir as pessoas que estavam no local, mesmo sem identificação de quem são num primeiro momento. Inicialmente o sistema segue um “objeto” (imagem sem definição do rosto) e, posteriormente, faz a identificação quando a face for visível, resolvendo um problema interessante de identificação posterior de um criminoso.

3.5 REDES NEURAIS

As redes neurais são estruturas computacionais que buscam simular o comportamento cerebral humano, a forma como aprendemos e principalmente como tomamos decisões baseadas neste aprendizado.

Formalmente uma rede neural é uma técnica eficiente para executar uma aproximação de uma função matemática. Ela tem uma grande capacidade de ser robusta e aprender a funcionar muito bem, mesmo em ambientes com muito ruído nas variáveis de entrada e ainda assim manter uma qualidade adequada e entregar resultados com boa precisão.

A parte central de uma rede é o perceptron, ele busca simular com a melhor precisão possível o funcionamento de um neurônio, basicamente ele é ensinado a responder em sua saída com 0 ou 1 a depender do valor de sua entrada, processando-a através de uma aproximação de uma equação matemática linear.

Uma rede neural é construída através da organização em camada de perceptrons, podendo ter diferentes camadas de perceptrons, dentro de cada camada e entre elas podem existir números diferentes de percetrons. As camadas podem estar parcial ou completamente conectadas.

Cada uma destas escolhas da arquitetura das redes neurais influenciará em suas características externas, como, por exemplo:

1) Velocidade de treinamento: para ensinar uma rede neural a aproximar o resultado de uma função, é preciso configurar cada um dos seus pesos dos perceptrons para que ao final possam responder adequadamente ao estímulo e assim classificar corretamente o sinal de entrada em uma saída. O processo de ensinar esta rede neural pode ser extremamente lento a depender da sua arquitetura interna, software utilizado para programar e principalmente o hardware responsável por executar este processamento;

2) Tempo de resposta a um estímulo: depois de treinada, a rede neural estará pronta para receber uma entrada e responder, baseada em seu treinamento, qual é a resposta correta para aquele sinal adquirido. Por razões parecidas com aquelas de velocidade para o treinamento, tais como arquitetura, software e hardware utilizados, acrescenta-se ao tempo de resposta o tipo de objeto enviado, por exemplo, uma imagem de altíssima resolução que será mais lentamente analisada do que uma imagem em escala de cinza de poucos pixels;

3) Precisão: a precisão, ou seja, a relação percentual de acerto entre a resposta gerada por uma rede neural e correta, também pode ser relacionada em grande parte à arquitetura escolhida. Não é possível obter resultados precisos em aproximações de funções complexas, como, por exemplo, classificação de imagens ou reconhecimento de voz, utilizando-se poucos perceptrons ou quando as camadas da rede não estejam completamente conectadas entre si.

4) Robustez: ter uma rede neural robusta significa que ela consiga funcionar bem mesmo quando o dado de entrada possua ruídos indesejáveis, como, por exemplo, uma fotografia distorcida ou com baixa luminosidade ou uma gravação de voz com ruídos sonoros externos que possam deixar a voz mais difícil de ser ouvida.

3.6 SVM (SUPORT VECTOR MACHINE)

É uma técnica computacional de aprendizagem de máquina supervisionada que organiza as entradas de dados, representando-os matematicamente como pontos em um espaço. A busca por estes pontos faz com que estes sejam representados o mais distante entre eles possível e tenta encontrar a função matemática que consiga separar as diferentes classes de dados em cada lado deste plano.

Para utilizar esta técnica é necessário que os dados estejam previamente classificados entre as classes possíveis.

A estratégia utilizada é buscar, dentre todas as possíveis funções que possam separar corretamente os pontos entre dois planos, aquela função que represente o plano e maximize a margem de segurança para tomada de decisão.

Desta forma é possível se utilizar a técnica SVM para o treinamento de análise de imagem, conseguindo classificar um exemplo entre possíveis classes previamente treinadas.

Existem alguns problemas conhecidos na utilização deste tipo de algoritmo de aprendizagem para classificação de imagens, quais sejam:

1) Não funciona bem para classificar imagens parecidas entre si, como, por exemplo, espécies de animais parecidos ou objetos similares com diferenças sutis, pois exige uma clara margem de separação entre eles;

2) Não funciona com conjunto de dados grandes para treinamento, pois uma parte importante do seu funcionamento é baseada em inversão de matrizes e este processo se torna muito lento conforme as matrizes crescem, inviabilizando o treinamento com bases de dados maiores que poderiam dar melhores exemplos para classificação;

3) Tem problema com a robustez, pois não é eficiente em lidar com eventuais ruídos nos dados de entrada, podendo ter a sua precisão rapidamente reduzida nestes casos, precisando utilizar em conjunto de outros algoritmos para fazer o pré-processamento das informações e submetê-lo para classificação com pouco ruído e as características de diferenciação mais claramente expostas para serem analisadas por ele.

3.7 CNN (CONVOLUTIONAL NEURAL NETWORK)

Existem diferentes algoritmos para detecção de informações em imagens, algumas delas vêm sendo utilizadas há muitos anos, principalmente a SVM, que utiliza estruturas computacionais muito eficientes em classificar imagens entre classes previamente definidas.

Estes tipos de estratégias são conhecidas como deep learning com treinamento supervisionado, visto que é preciso um trabalho de treinamento com objetos previamente classificados naquelas classes que existe interesse.

Por exemplo, se é necessário ensinar uma rede neural a detectar se uma determinada imagem contém um gato ou um cachorro, é preciso ensiná-la utilizando diversos exemplos de cada uma destas classes.

Um dos principais desafios é a obtenção destas bases de imagens categorizadas para treinamento. Atualmente na internet existem diversas bases de imagens categorizadas e tagueadas para uso em pesquisa científica.

O grande avanço deste tipo de redes é sua capacidade de sintetizar as características principais das imagens, retirando itens de pouco impacto na análise completa da imagem.

São aplicados filtros iniciais nas imagens para retirar ruídos e deixar somente os elementos mais representativos, tais como bordas, vértices, formas geométricas, mudanças relevantes de cores dentro ou fora do mesmo objeto. Com esta característica é possível aumentar significativamente a robustez dos resultados obtidos por ela.

Outra característica é a convolução, com esta técnica é possível reduzir significativamente o tamanho da matriz de dados a serem trabalhados sem impactar relevantemente no resultado obtido por ela.

Com esta técnica ganham-se duas características desejáveis para as redes neurais, o seu tempo de treinamento é significativamente reduzido e o tempo de resposta também é muito rápido, permitindo seu uso em aplicações de análise de imagem em tempo real.

Mesmo com uma quantidade significativamente menor de imagens de exemplos, a precisão tende a ser maior do que a abordagem SVM, pois ela consegue perceber mais eficientemente as características que permita diferenciar com melhor qualidade um objeto entre todas as possíveis tipos de classificação.

Por estas vantagens é recomendável a utilização desta tecnologia na análise dos vídeos para a detecção de eventos especiais, como, por exemplo pessoas caídas, focos de incêndio, acidentes.

Este tipo de imagens possui características claramente definidas e que podem ser ensinadas a uma rede convolucional que terá a capacidade de generalizar da melhor forma suas características mais importantes para que possa utilizar este aprendizado em seu processo de monitoramento.

A excelente capacidade de generalização da CNN é uma das suas melhores características para utilização em uma cidade inteligente, pois com centenas ou em alguns casos, milhares de câmeras capturando imagens de diferentes ambientes, eventos similares, como, por exemplo um acidente de trânsito gerará imagens graficamente muito diferentes entre si, porém características similares podem ser extraídas delas, mesmo em condições muito diferentes de cores e objetos de fundo na cena.

É a capacidade de “perceber” que um acidente pode ser representado por um evento de colisão entre dois automóveis, ou mesmo um ou mais veículos parados em uma via onde é esperado que o tráfego esteja fluindo normalmente, ou mesmo o padrão de carros desviando de um determinado ponto da rodovia, reduzindo a velocidade e estrangulando o trânsito em um ponto específico.

Ou ainda, o caso de uma pequena aglomeração de pessoas em uma calçada, em volta de um objeto, que pode ser uma pessoa caída ou ferida, gerando um alerta. As calçadas, lojas e casas fazem a cena variar significativamente e a capacidade de extrair as características que de fato representem o evento a ser reconhecido é muito importante. Para que esta capacidade de generalização seja atingida é preciso treinar o modelo com muitas imagens de situações diferentes e seu tempo e custo de retreinamento não pode ser lento em razão disso.

Ter uma rede CNN analisando as imagens das inúmeras câmeras de uma cidade inteligente é como ensiná-las implicitamente em quais informações ou elementos devam prestar atenção e quais são irrelevantes para a finalidade que foram implementadas.

Outra característica muito útil no caso de uso em cidades inteligentes é sua robustez frente aos ruídos gerados, principalmente resolução das imagens, foco e luminosidade, que obrigam trabalhar em situações não ideais de entrada de dados.

A construção de um sistema robusto é um dos mais importantes objetivos da Engenharia de Computação, pois permite que ele continue prestando seus serviços mesmo em situações adversas e não testadas previamente em tempo de projeto, pois seria impossível simular e prever todas as possíveis situações nas quais o sistema irá se deparar em produção.

3.8 DETECÇÃO DE EVENTOS

Os sistemas de detecção de objetos podem ser treinados para identificar situações de alertas importantes, aumentando ainda mais a segurança das cidades inteligentes, como, por exemplo:

– Incêndios: identificar nas imagens padrões de fogo e fumaça e gerar um alerta específico para o Corpo de Bombeiros. É possível identificar as chamas por meio do seu formato e movimentos específicos e principalmente cores. Outra característica importante e que pode ser utilizada para a correta identificação de um foco de incêndio é a fumaça, também por sua forma e cores (YU, 2013). A utilização da forma e do padrão irregular da movimentação das chamas é muito importante para reduzir os falsos positivos que acabam acontecendo por causa de objetos de cores muito intensas (MUHAMMAD, 2018);

– Semáforos com problema: identificar que eles estejam piscando amarelo intermitente e acionar a companhia de controle de tráfego;

– Alagamentos: verificar uma quantidade grande de água em locais onde não deveria haver;

– Pessoas perdidas: os desaparecidos podem ser mais rapidamente encontrados ou efetua-se uma busca pelo último lugar e horário onde foram vistos;

– Acidentes de carro: identificar veículos colididos, acidentados ou parados em acostamentos com informe às autoridades responsáveis;

– Pessoas acidentadas: é possível acionar os serviços médicos de emergência;

– Aglomerações: é possível perceber que existe uma quantidade grande pessoas em determinado ponto e tomar atitudes preventivas em lugares que possam gerar perigo, como uma estação de metrô, por exemplo;

– Aglomerações de veículos: identificar se uma certa quantidade de veículos está trafegando junta há algum tempo por diferentes pontos da cidade;

– Animais: encontrar animais nas ruas sem o seu responsável pode significar uma situação de alerta;

– Contagem de pessoas: possibilidade que se torna útil para destinar dinamicamente os serviços de transporte público, enviando mais ônibus e trens nas linhas de maior demanda momentânea, fazendo assim uma gestão mais eficiente dos recursos disponíveis.

3.9 HISTÓRICO

É importante que um sistema de monitoria por imagem de uma cidade inteligente seja capaz de buscar todas as situações anteriores em que aquela face foi reconhecida.

Muitas vezes é preciso encontrar evidências da presença de uma pessoa em um determinado local, por exemplo, para reforçar ou negar o álibi de um suspeito de um crime no qual existam dúvidas sobre a sua localização em um determinado momento no tempo.

Outra situação igualmente relevante é na busca por pessoas desaparecidas. Nestes casos, normalmente é possível utilizar o momento de partida como sendo o último local e horário onde a pessoa foi vista por alguém confiável e a partir dali iniciar uma busca pela sua aparição em diferentes câmeras no sistema.

Neste caso é possível identificar o que aconteceu de fato com a pessoa que está sendo procurada ou mesmo se eventualmente ela tenha sido encontrada em algum veículo que possa então vir a ser procurado através de sua placa de identificação.

Para ser possível executar esta função é preciso manter as imagens do período escolhido disponíveis para o sistema fazer uma busca reversa, procurando encontrar aquela pessoa nas imagens anteriores.

Os custos de armazenagem em disco são proporcionais ao tempo de armazenagem histórica de imagens, ou seja, quanto maior for a armazenagem, maiores seus custos. Por este motivo é muito relevante a aplicação de um estudo de casos anteriores onde estas buscas foram solicitadas para a definição de um período suficientemente longo para permitir o uso efetivo, porém não tão longo

que possa gerar custos desnecessários por guardar históricos que nunca serão utilizados de fato.

Além disso, no momento do acionamento da busca histórica em si, uma imensa quantidade de processamento será exigida para que possa processar no menor prazo possível todas as imagens arquivadas.

Para que seja viável executar este processo de forma eficiente é interessante que o sistema seja implementado com as seguintes características:

– Processamento Paralelo: é a capacidade de processar simultaneamente mais de uma imagem, dividindo as tarefas e executando-as em processadores diferentes ao mesmo tempo;

– Assincronicidade: permitir que a análise de cada imagem não dependa de uma resposta anterior, ou seja, que possam ser trabalhadas independentemente e seu tempo de resposta não afete os processamentos posteriores;

– Exclusão de duplicidade: quando diferentes frames de um vídeo são analisados, é bastante comum que em diversos frames sequenciais, as pessoas identificadas sejam as mesmas. Perceber esta informação é muito importante para minimizar a tarefa computacional de inspecionar estas faces identificadas;

– Eliminação de indivíduos já identificados previamente: aqueles indivíduos que já tenham sido identificados pelo sistema em seu banco de dados não devem ser ressubmetidos ao procedimento de busca por uma pessoa nova.

3.10 TRACKING

Em monitoramento por imagem, uma das funções mais importantes certamente é a capacidade de tracking da pessoa identificada, ou seja, a capacidade de marcar uma face e passar a segui-la nas câmeras onde ela possa aparecer posteriormente.

Existem algumas situações em que esta funcionalidade possa ser importante, como, por exemplo, um assalto a banco ou a uma loja. A partir de uma detecção de emergência, o sistema poderia seguir para onde foram pessoas que estavam no local, mesmo sem identificá-las num primeiro momento.

Pode-se assim obter a interessante função de identificação *a posteriori* de um criminoso.

Inicialmente o sistema seguirá um “objeto” (imagem sem definição ainda de face) e, em algum momento posterior, quando a face for visível, fará a identificação precisa.

Este funcionalidade é muito utilizada nas seguintes situações:

– Interceptar uma pessoa fisicamente: quando um suspeito ou desaparecido é identificado, solicita-se que os responsáveis sejam deslocados até o ponto para encontrar a pessoa em questão. Durante este período é importante monitorar para garantir que a pessoa não seja perdida até que eles a encontrem;

– Monitoramento de um comportamento suspeito: acompanhar uma pessoa identificada em um comportamento estranho até que alguma nova ação possa ser definida, seja ela pela interceptação ou descarte deste acompanhamento.

É possível otimizar significativamente o processo de tracking de uma pessoa em diferentes câmeras se houver um mapa físico do posicionamento geográfico de cada equipamento.

Assim é possível inferir a provável nova aparição e localização posterior em uma imagem quando a pessoa sair de foco por um determinado lado da imagem, evitando-se assim uma varredura ampla entre todas as demais câmeras do sistema, o que causaria uma quantidade grande de processamento desnecessário.

3.11 CONTAGEM DE PESSOAS

Outra função útil de um sistema de monitoramento da cidade inteligente é a contagem de pessoas em determinados lugares. Acompanhar estas quantidades e compará-las com os valores médios históricos permite gerar alertas para situações especiais, tais como:

– Acidentes: normalmente o número de pessoas se altera significativamente em locais que tenham ocorrido acidentes, seja aumentando em razão da curiosidade ou diminuindo pelo medo de uma situação potencialmente perigosa;

– Lentidão no transporte público: aglomeração de pessoas em locais de embarque como estações e terminais, gerando situações de risco que precisem ser acompanhadas pelos responsáveis e também permitindo que ações de reorganização de frotas e intervalos entre ônibus e trens possam ser modificados para fazer frente à demanda incomum;

– Protestos: manifestações políticas normalmente contam com um número grande de pessoas em uma alta densidade, muitas vezes em locais de grande fluxo de veículos, exigindo assim a imediata gestão do trânsito e da segurança para permitir que o direito democrático de todos seja resguardado de forma organizada.

Para que o sistema de alerta funcione bem é preciso construir um banco de dados histórico relativamente preciso, levando em consideração os momentos de picos pontuais, como, por exemplo, saída e entrada de alunos em escolas, horários de maior uso de transporte público, jogos e atividades esportivas, diferença entre dias úteis e dias de descanso, etc.

Com estas informações corretamente cadastradas e consolidadas no sistema, os alertas tenderão a ser muito precisos, ajudando na organização do monitoramento físico dos pontos da cidade que precisem de maior atenção naquele momento.

3.12 ILUMINAÇÃO E SEGURANÇA

A iluminação pública é essencial para a qualidade de vida nas cidades, sua principal função é estender a iluminação diurna à noite.

Os fatores essenciais da iluminação pública são:

– Promover visibilidade de objetos;

– Dar sentido e orientação ao longo das vias;

– Deixar as cidades mais atraentes e permitir seu uso pleno à noite;

– Prover segurança pública.

Para contextualizar a importância da iluminação no dia a dia e a sua influência na segurança pública, é necessário voltar no tempo e entender os processos da sua evolução.

Desde a era medieval os seres humanos buscam resolver os problemas de iluminação com o uso de velas e principalmente tochas com fibras vegetais e embebidas com diversos tipos de material inflamável (MARTINS, 2011).

Em 1415, na Inglaterra, surgem as primeiras instalações de iluminação urbana que tiveram como princípio básico o objetivo de reduzir a violência e os frequentes roubos aos comerciantes.

Até o século XIX e início do século XX, as lâmpadas a gás foram utilizadas em larga escala, logo elas foram substituídas pelas lâmpadas elétricas. Em 1854 surge a primeira lâmpada desenvolvida de fibras de bambu e ampolas de vidros transparentes, criada pelo mecânico alemão Johann Heinrich Goebel (1818-1893).

A criação do dínamo surgiu em 1867, realizado pelo engenheiro Werner Siemens, o que possibilitou o uso industrial da eletricidade. Em 1879, Thomas Edison, mediante várias tentativas conseguiu melhorar as lâmpadas incandescentes e torná-las mais resistentes e duráveis. Em 1882, Nova Iorque foi a primeira cidade do mundo a ter iluminação pública gerada por uma termelétrica.

Até o século XVIII, não existia iluminação pública no Brasil. Em 1794 foram instaladas cerca de 100 luminárias a óleo de azeite pelos postes da cidade do Rio de Janeiro.

Segundo Rosito (2009), a inovação na iluminação pública surgiu quando na cidade de Campos, no Rio de Janeiro, uma máquina a vapor foi utilizada para iluminar o distrito com 39 lâmpadas.

Em 1887, em Porto Alegre, uma usina elétrica começa a operar, dando origem ao primeiro serviço municipal de iluminação elétrica.

No século XX ocorreu uma grande evolução no setor de geração de energia no Brasil, consequentemente houve um avanço significativo também na iluminação pública.

A iluminação pública está diretamente ligada à qualidade de vida das pessoas; ambientes públicos bem iluminados permitem aos habitantes desfrutarem desses espaços em horários diurnos e noturnos, pois reduzem a criminalidade, favorecem a integração entre as pessoas, embelezam as cidades atraindo o turismo e trazem lucratividades para os comércios locais.

Os principais objetivos para iluminar os ambientes públicos, à noite, é alcançar as expectativas sociais ou econômicas, que incluem segurança, auxílio ao desenvolvimento, e notoriedade às áreas históricas ou espaços verdes públicos. Ruas bem iluminadas dão a sensação de segurança aos pedestres, pois aumentam a visibilidade, podendo supostamente desanimar os criminosos (MASCARO, 2006).

Uma prova disto é um fato histórico reportado por Aver, na Inglaterra, em 1974, durante a crise do petróleo, quando a iluminação pública foi reduzida em 50% em algumas áreas urbanas, as estatísticas apontaram o aumento de 100% nos indicadores de furtos e de 50% nos índices de criminalidade. Partindo do princípio de que a escuridão é aliada do criminoso, pode-se afirmar que a iluminação pública e a segurança estão muito relacionadas.

Existem vários autores que relacionam a ausência de iluminação como um ambiente propício a configurações de ocorrências criminais, entre eles pode-se citar Roizenblatt (2009), Marchant (2010) e Farrington e Welsh (2003).

Além da redução da criminalidade, uma iluminação de qualidade é capaz de criar prioridades de percepção do espaço à noite. Na Figura 1 pode-se

observar a estufa do Jardim Botânico destacando-se devido à sua iluminação diferenciada.

Figura 1 – Estufa com iluminação diferenciada (Jardim Botânico – Curitiba)
Fonte: Wiki Commons (2009).

A ABNT padroniza o sistema de iluminação pública brasileiro, porém as concessionárias de energia elétrica também possuem seus próprios padrões normativos, contudo sem sobrepor as recomendações das normas técnicas brasileiras.

Em 2000, a ANEEL, por meio da Resolução Normativa n° 414, de 9 de setembro de 2010, em seu artigo 218, definiu que a responsabilidade de ampliação e manutenção da iluminação das vias públicas passou a ser da prefeitura, as concessionárias de energia local são responsáveis apenas pelo fornecimento de energia elétrica (ANEEL, 2015).

Dois critérios foram escolhidos como determinantes e padronizados para garantir a qualidade da iluminação de vias públicas:

– Nível de iluminância;

– Fator de uniformidade de iluminância.

Segundo Tregenza e Loe (2015), a iluminância é a quantidade de luz incidente em uma superfície e é medida com o número de lumens em uma unidade de área de superfície. A unidade do Sistema Internacional de Unidades, é o lúmen por metro quadrado, que, por questões práticas recebeu o nome de *lux*. A iluminância também pode ser associada à percepção que o ser humano tem do brilho de uma área iluminada.

De acordo com a importância, tipo e volume de tráfego noturno da via, são recomendados valores que variam de 2 a 20 lux para o nível de iluminância, e de 0,2 a 0,5 para o fator de uniformidade, que é a relação entre a iluminância mínima e média de uma determinada área (ABNT, 1992).

Um problema importante do sistema de iluminação pública é que seu funcionamento se inicia juntamente durante o horário de pico de consumo, pois estão funcionando concomitantemente indústrias, a iluminação pública e residencial, além de eletrodomésticos e chuveiros, o que implica em adoções de programas de melhorias de eficiência, a fim de otimizar os investimentos na redução do consumo da energia elétrica.

As oportunidades para a eficiência energética na iluminação pública, de acordo com Castro e Luciano (2012), são:

– Redução das despesas com consumo de energia;

– Redução dos custos com manutenção e pessoal;

– Facilidade operacional de implantação e manutenção;

– Melhoria da imagem turística das cidades;

– Postergação de investimentos no sistema elétrico;

– Redução dos impactos socioambientais.

Desta forma, é de interesse dos responsáveis pela segurança e manutenção dos ambientes públicos, terem informações atualizadas sobre a

qualidade da iluminação pública, ou seja, a quantidade de luz refletida em uma determinada área em tempo real.

Note-se que o termo luminosidade difere de iluminação, pois é possível manter o mesmo nível de segurança caso ocorra uma falha no sistema de iluminação se ainda existir luz natural do dia ou de outras fontes, como um painel publicitário, por exemplo.

O processo que faça a integração entre iluminação pública e segurança deverá levar em consideração que, em alguns casos, existem áreas da cidade que praticamente não recebem iluminação natural (ruas estreitas, por exemplo) e, nestes casos, uma falha na iluminação, mesmo durante o dia, pode modificar o mapa de oportunidade para um criminoso.

Alguns pontos de iluminação pública podem conter sensores de luminosidade acoplados, responsáveis por medir a intensidade da luz em um determinado local e ativar ou desativar a iluminação pública dependendo do grau de luminosidade. Em locais que já possuem esse dispositivo, é mais simples fazer um controle cruzando a luminosidade natural e a luminosidade total (luminosidade natural somado à luminosidade artificial obtida através do uso de lâmpadas, caso estas estejam acionada).

Existem casos onde se perde a comunicação completa com um ponto de iluminação (sensor de luminosidade e lâmpada). Neste caso é necessário ter um mapeamento de qual outro ponto pode ser usado como fonte de aproximação temporária para estimar a informação não disponível.

No caso de pontos de iluminação sem sensor de luminosidade, condição essa bastante comum nas grandes cidades, será necessário estimá-la baseado em informações meteorológicas disponíveis, obtendo um resultado com uma precisão menor (por causa de possíveis sombras naturais, como nuvens, ou artificiais, como prédios), porém ainda assim bastante útil para o objetivo inicial.

Com ambas informações disponíveis pode-se trabalhar sistematicamente da seguinte forma:

1) Percorrer recorrentemente todos os pontos de iluminação obtendo os dados sobre o nível de luminosidade natural;

2) Para aqueles pontos que estejam abaixo do limiar definido como seguro, verificar se a lâmpada está acesa;

3) Caso a lâmpada não esteja funcionando, gerar um alerta para a companhia responsável pela iluminação pública solicitando o conserto;

4) Se a área em questão tiver histórico de ocorrências criminais, o sistema deve gerar uma notificação e aumentar os indicadores até o próximo ponto de iluminação que esteja sabidamente funcionando de maneira correta;

5) Solicitar uma equipe tática para que se desloque ao ponto para avaliar presencialmente as condições, e verificar se é necessário permanecer no local até o término do reparo técnico;

6) Em caso de recorrência da ausência de luminosidade no local, devido a danos no equipamento, deve-se iniciar uma investigação técnica e policial para verificar se existe algum fator externo influenciando, seja ele um problema elétrico ou mesmo alguém mal-intencionado danificando o equipamento propositadamente.

3.13 SEGURANÇA E PRESENÇA HUMANA

Outra circunstância que possui um grande impacto na mudança de oportunidade é a ausência de um funcionário responsável pela segurança de um determinado posto fixo, como uma guarita, por exemplo.

O sistema deverá ser capaz de identificar se um determinado posto está desguarnecido ou não, através de sensores capazes de detectar a movimentação de fontes de calor utilizando infravermelho ou câmeras de segurança. Caso o sistema seja informado que um posto esteja desguarnecido, pode-se atuar da seguinte forma:

– Gerar um chamado para a empresa responsável para saber o motivo, se o problema é uma falta simples ou se o funcionário pode estar em uma situação de coação física;

– Se a área em questão tiver histórico elevado de ocorrências criminais, considerando-a como um local perigoso, o sistema deve gerar uma notificação e aumentar os indicadores do setor sob a gestão daquele segurança;

– Solicitar que uma equipe tática se desloque ao ponto para avaliar pessoalmente as condições e verificar se é necessário permanecer no local até a reposição do funcionário.

3.13.1 Análise Criminal

A análise criminal teve origem nos Estados Unidos da América, no final da década de 1920, quando os xerifes da Associação dos Chefes de Polícia (International Association of Chiefs of Polices – IACP) propuseram a criação de grandes bases administrativas de dados agregados referentes à criminalidade, conforme relata Dantas (2016, p. 2).

> Tais bases de dados teriam grande abrangência, não só territorial, mas também “histórica”, cobrindo vários anos, o que veio a chamar-se, nos EUA, de “Uniform Crime Report System” (Sistema de relatórios Padronizados à Criminalidade – UCRS). A atual “tecnologia do conhecimento criminológico”, elaborada a partir de dados produzidos pelo UCRS nos EUA, está hoje incorporada ao acervo formal do conhecimento acadêmico.

É um processo analítico e sistemático de produção de conhecimento, orientado segundo os princípios da pertinência e da oportunidade, sendo realizado a partir do estabelecimento de correlações entre um conjunto de fatos delituosos ocorridos (“ocorrências policiais”) e os padrões e tendências da “história” da criminalidade de um determinado local ou região (DANTAS, 2016).

Esta atividade é a decomposição do incidente em partes menores constituintes, dos efeitos e das causas.

Na atuação policial, a análise criminal procura as causas da criminalidade, através do estudo de seus efeitos, trabalhando muitas vezes de forma reversa aos fatos cronologicamente ocorridos; procura decompor os fatores e estudá-los de forma detalhada e separadamente, no aspecto qualitativo e quantitativo.

A análise quantitativa verifica a proporção de fatores e variáveis que influenciam no comportamento criminal, em abordagem numérica e de fácil interpretação.

Já a análise qualitativa identifica os fatores e as variáveis que influenciam no comportamento criminal, sendo um dos processos mais complexos em que o responsável deve entender a relação que os fatores têm com o comportamento entre si. A análise qualitativa ajuda a definir melhor o problema a ser solucionado.

Dantas (2016) aponta alguns fatores condicionantes do crime e da criminalidade, que são:

1) Densidade populacional e grau de urbanização local, bem como o tamanho da comunidade e de suas áreas adjacentes;

2) Variação na composição do contingente populacional local, particularmente quanto à prevalência de estratos populacionais jovens e de indivíduos do sexo masculino;

3) Estabilidade da população no que concerne à mobilidade de residentes locais da comunidade, seus padrões diários de deslocamento e presença de população transitória ou de não residentes;

4) Meios de transporte localmente disponíveis e sistema viário local;

5) Condições econômicas, incluindo renda média, nível de pobreza e disponibilidade de postos de trabalho;

6) Aspectos culturais, educacionais, religiosos e oportunidades de lazer e entretenimento;

7) Condições da matriz social nuclear, em relação ao divórcio e coesão do grupo familiar;

8) Clima local;

9) Efetividade das instituições policiais locais;

10) Ênfase diferenciada das polícias locais nas funções operacionais e administrativas da instituição;

11) Políticas, métodos e processos de funcionamento das outras instituições que dão corpo ao sistema local de justiça criminal, incluindo o Ministério Público, Poder Judiciário e Autoridade Prisional;

12) Atitudes da cidadania em relação ao crime;

13) Práticas prevalentes de notificação de delitos ocorridos às autoridades policiais.

3.14 PREVENÇÃO

As ações preventivas da criminalidade devem ser adotadas extensivamente pelos responsáveis pela gestão da segurança pública, pois além de mais barata é também muito mais eficiente no longo prazo para a melhoria da qualidade de vida dos cidadãos.

O foco deste trabalho deve ser nos fatores de tempo, espaço, modo de atuação do cidadão infrator e tipo de crime.

A ação policial deve ser aplicada com a correta alocação dos recursos logísticos e potencial humano para uma prevenção eficiente e eficaz.

3.14.1 Prevenção Situacional

O conceito de policiamento operacional padrão (POP) foi introduzido por Herman Goldstein em um ensaio publicado em 1979, cujo marco teórico traz como objetivo do policiamento a ação sobre as causas que dão origem aos problemas de segurança repetitivos, e não simplesmente responder aos incidentes quando eles ocorrem ou tentar impedi-los por meio de policiamento ostensivo (CLARKE; ECK, 2005).

Para minimizar a ronda policial, Goldstein (1979) sugere que a polícia utilize as seguintes etapas:

– Exame cuidadoso dos dados, para identificar padrões dos incidentes com os quais a polícia lida rotineiramente;

– Análise profunda das causas desses padrões (ou problemas);

– Descoberta de novas formas de intervir previamente na cadeia causal, a fim de reduzir a probabilidade de ocorrência desses problemas no futuro;

– Avaliação de impacto das intervenções e, se elas não tiverem sucesso, iniciar o processo novamente (CLARKE; ECK, 2005).

3.15 MAPA DE CRIMINALIDADE

Para criar um mapa de criminalidade atualizado, que será o resultado do processamento dos dados inseridos no sistema especialista, é primordial realizar a cuidadosa definição dos dados que serão cadastrados, a fim de que após o processamento destas variáveis, o sistema traga informações confiáveis para os gestores.

Atualmente existem sistemas que agrupam informações sobre a criminalidade, tais como o sistema inteligente de Registro Digital de Ocorrências (RDO) e de informações criminais (INFOCRIM), que possibilitam aos policiais verificarem os bairros com os maiores índices de criminalidade.

Uma observação interessante é que em sua grande maioria não há integrações entre as bases estaduais, pois as polícias no Brasil estão subordinadas aos Estados.

A tecnologia é de grande importância para ajudar as investigações policiais, auxiliando no policiamento ostensivo e principalmente preventivo.

4 SEGURANÇA E BIG DATA

Big data é um termo utilizado para descrever um conjunto de dados armazenados, estruturados ou não, que impactam no dia a dia das pessoas.

Podemos dividir os dados não estruturados em:

– Dados não estruturados simples: são informações que não estão organizadas, muitas vezes contêm dados irrelevantes e em alguns casos repetidos, dificultando a sua interpretação através de um banco de dados;

– Dados multiestruturados: são dados gerados através de várias fontes, que possuem estruturas diferentes e agrupados desordenadamente, com possíveis inconsistências e sobreposições.

Os dados em si não possuem muito valor, o que agrega valor para as empresas são as informações coletadas a partir da análise destes dados. Estas informações poderão auxiliar na tomada de decisão, na redução de custos, na identificação da causa raiz de falhas, na detecção de comportamentos suspeitos ou fraudulentos, entre outros (SAS, 2016).

A definição do Big Data utilizando os 3 Vs, termo criado pelo analista Doug Laney (SAS, 2016), é:

– Volume: dados são coletados de diversas fontes gerando um conjunto de informações que precisam ser armazenadas. O que no passado era um problema, atualmente existem novas tecnologias que têm conseguido responder bem a esta necessidade;

– Velocidade: os dados são gerados em uma velocidade sem precedentes e devem ser tratados em tempo hábil. Sensores celulares e contadores inteligentes estão impulsionados à necessidade de lidar com esta massa de dados em tempo real;

– Variedade: não existe uma padronização dos dados, eles são gerados em todos os tipos e formatos de dados estruturados, dados numéricos em

banco de dados tradicionais, até documentos de textos não estruturados, e-mail, vídeo, áudio, dados de cotações da bolsa e transações financeiras.

O Big Data será utilizado no sistema especialista para armazenar e processar os dados recebidos de diversas fontes. Estas informações serão importantes para auxiliar os responsáveis pela segurança a realizarem ações preditivas através de informações geradas a partir da análise de dados capturadas de diversas fontes, inclusive de redes sociais.

Será criado um algoritmo capaz de realizar uma análise estatística dos dados históricos e dados recebidos em tempo real, e através desses dados irá mapear os pontos inseguros, onde existe a possibilidade de ocorrer algum tipo de ocorrência criminal.

4.1 SEGURANÇA DA INFORMAÇÃO

Por ter uma grande importância econômica e social, este tipo de sistema tem se tornado cada vez mais visado para ataques.

Atualmente, somente no Brasil, os crimes cibernéticos são responsáveis por um gasto de US$ 10 bilhões feito pelas empresas, segundo informa a notícia veiculada em sites relacionados à segurança (REVISTA VEJA, 2018).

Manter o sistema protegido em relação às principais ameaças conhecidas é a melhor forma de manter o sistema afastado de um ataque.

A organização mundial sem fins lucrativos Open Web Application Security Project (OWASP) mapeia e divulga as principais ameaças a sistemas de internet, dessa forma, todos podem conhecê-las e assim podem trabalhar para minimizar estas possíveis falhas que favorecem o ataque aos dados sensíveis do site ou dos usuários.

O Brasil é o segundo país em quantidade de capítulos da OWASP, atrás apenas dos EUA (CARVALHO, 2014), demonstrando que a preocupação com a construção de sistemas mais seguros já se faz presente no país.

Segundo a OWASP, alguns dos principais tipos de ataques foram:

1) Injeção: introdução de informações indevidas por entradas de dados não tratados para manipulação de comandos e a consequente captura de

dados sem a devida autorização. Esta técnica tem sido amplamente utilizada para capturar dados sensíveis de sites com grande base de usuários e seu impacto, tanto na imagem da empresa quanto financeiramente (mediante compensações judiciais) é dispendioso;

2) Erro de autenticação e controle de sessão: atribui-se a não realização correta das funções de controle de autenticação e de sessão, concedendo que o atacante aceda a senhas, tokens e em alguns casos aproprie-se da identidade de outros usuários verdadeiros. Pode promover atos que venham a causar prejuízos tanto à empresa quanto ao usuário real, permitindo que um usuário se utilize de outra identidade;

3) Cross-Site Script (XSS): quando o sistema web recebe informações do atacante e não os trata adequadamente, permite que este mande instruções que serão replicadas pelo sistema para os demais usuários, favorecendo uma série de ações maliciosas como roubo de dados e redirecionamentos indevidos. O usuário legítimo acaba tendo o maior prejuízo, uma vez que sem poder identificar que foi manipulado, pode entregar informações sigilosas ou sensíveis para o atacante no segundo momento e este utilizá-las para outros fins;

4) Observações inseguras a objetos: permite que o atacante manipule a direção do objeto que seria enviado, por exemplo, um arquivo, e solicite outro em seu lugar que deveria ser sigiloso. Em alguns casos este ataque pode ser feito para tentar obter mais informações de um ambiente de infraestrutura (por exemplo, versões de softwares e bibliotecas), planejando um ataque posterior mais eficiente;

5) Erros de configuração: execução incorreta das configurações de segurança sugeridas pelo fabricante ou comunidade de usuários (bastante comuns em softwares livres) e necessárias para o perfeito funcionamento dos mecanismos do Sistema Operacional, Webserver, Banco de Dados, Linguagem de Programação, Framework, etc.;

6) Revelação de dados significativos: a falta de resguardo adequado dos dados importantes de usuários por meio de criptografia tanto no arquivamento quanto no envio, tais como senhas, números de cartão de crédito, número de documentos, endereços, etc., faz o atacante conseguir utilizar a técnica de injeção naquele sistema, assim, os resultados podem ser devastadores para a empresa em questão, pois o acesso seria completo e o impacto é incomensurável;

7) Ausência de moderação de acesso: a moderação realizada somente na interface web sem a devida replicação na camada de acesso aos dados no servidor pode facilitar com que o atacante manipule a interface e assim solicite dados que ele não deveria ter acesso por seu nível de permissão. O prejuízo dependeria do quanto este usuário conseguisse obter de acessos extras, mas em geral o prejuízo é para a empresa com a redução da geração de receita, por exemplo, quando um atacante consegue ter acesso a uma conta “premium” quando contratou um serviço “basic”;

8) Cross-Site Request Forgery (CSRF): possibilidade de incentivar o usuário corretamente autenticado a enviar dados para um servidor diferente, por se passar pela aplicação legítima. Os efeitos são parecidos com o Cross-Site Script (XSS), no entanto, em alguns casos o atacante não necessita descobrir novamente em um segundo momento, pois ele já tem as informações que necessita no primeiro passo do ataque ao usuário real;

9) Usar elementos conhecidos por sua vulnerabilidade: consentir a continuidade de manter em produção softwares vulneráveis sem a sua atualização para a versão mais recente, em que estas já tenham sido minimizadas. De modo geral, esta situação acontece por dois motivos: ausência de processos atualizados de governança da infraestrutura, em que os responsáveis acompanham os fornecedores dos sistemas ou quando existe obsolescência do software principal que se torna dependente de componentes antigos para continuar funcionando, por exemplo, bibliotecas de código;

10) Invalidação de redirecionamentos: permissão aos usuários do sistema para que sejam redirecionados inadvertidamente ou mesmo de forma indevida para outros sistemas que possam solicitar-lhes dados de maneira explícita ou transparente. Os efeitos também são similares ao Cross-Site Script (XSS), entretanto, o atacante muitas vezes não precisa nem mesmo de grande conhecimento técnico, por isso mesmo, é um ataque bastante simples de ser defendido.

Pessoas treinadas para perceberem ataques conseguem antevê-los, diferentemente daquelas que hoje utilizam largamente computadores conectados à rede, mas que não possuem conhecimentos suficientes para perceberem ataques.

Muitas empresas sem equipes ou fornecedores capacitados têm colocado sistemas críticos para funcionamento sem o devido respaldo necessário para suportar corretamente o nível de qualidade exigido por seus usuários e defender adequadamente os ativos sob sua gestão.

O número do incidentes reportados pelo CERT.br mais do que quintuplicou nos últimos 10 anos.

A Figura 2 mostra a evolução histórica destes incidentes:

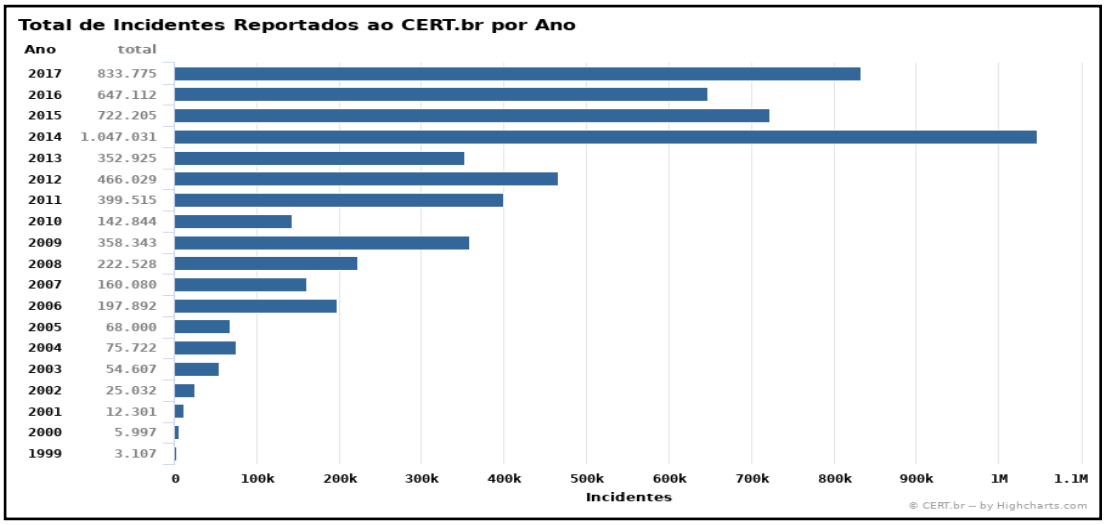

Figura 2 – Incidentes Reportados pelo CERT.br (2018)
Fonte: CERT.br (2019).

Grande parte destes incidentes são domésticos, entretanto, pode-se identificar uma quantidade significativa de eventos vindos dos EUA e China.

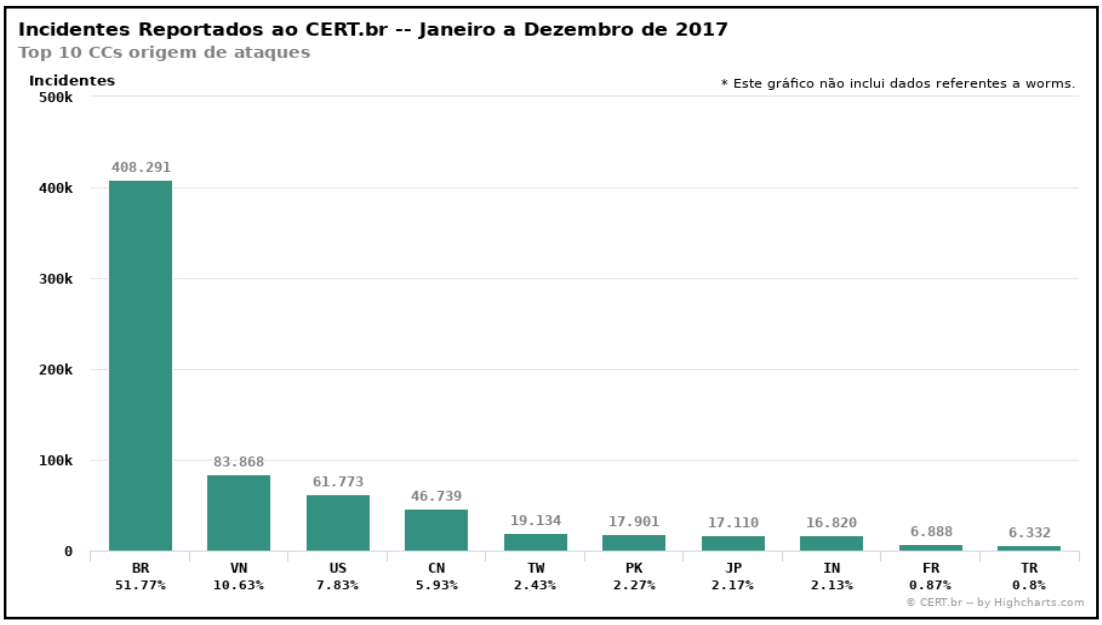

Figura 3 – Incidentes Reportados por país de origem pelo CERT.br (2018)
Fonte: CERT.br (2019).

Construir um sistema seguro é um trabalho complexo e necessita ter um processo de desenvolvimento maduro, usar os melhores componentes e, principalmente, uma equipe bem treinada teórica e praticamente nos quesitos de segurança de software.

As instabilidades dos softwares, na maioria das vezes, compreendem o processo de desenvolvimento de modo geral. Prazos curtos de entrega das aplicações juntamente com processos vulneráveis resultam em maior taxa de falhas de segurança (MONTEVERDE; CAMPIOLO, 2014).

Algumas das principais contramedidas que podem ser adotadas pela empresa responsável pelo desenvolvimento para se obter um sistema de melhor qualidade no quesito segurança estão abaixo listadas:

– Utilizar uma boa infraestrutura, com a análise cuidadosa do histórico do Datacenter contratado, Sistema Operacional, Webserver, Banco de Dados e Bibliotecas de Código. Aconselha-se estar presente e acompanhamento regular das listas de discussões por e-mail sobre segurança de todos eles;

– Configurar o firewall de modo correto, com a aplicação de módulos construídos para detectar as invasões mais comuns, conforme Akbar e Ridha (2018) e possivelmente utilizando Machine Learning para aperfeiçoamento da capacidade de detecção de ocorrências suspeitas, como citado por Betarte, Pardo e Martínez (2018);

– Preparar a equipe para que ela tenha segurança como um fator primordial de qualidade e saiba programar de forma adequada o sistema conhecendo as técnicas e teorias principais fundamentais do tema. De acordo com Souza (2012), o maior objetivo deve ser a redução da chance dos desenvolvedores introduzirem de modo involuntário vulnerabilidades de segurança, usando as boas práticas de desenvolvimento, como a validação de entradas a fim de verificar se os dados de entrada estão no padrão esperado pela aplicação; e tratamento de exceções, para controlar alterações na sua movimentação normal;

– Utilizar uma boa linguagem e framework de programação com segurança como um dos objetivos primordiais em sua arquitetura;

– Possuir uma equipe de qualidade treinada para rastrear sistemas de segurança de forma constante, utilizando softwares referência de mercado;

– Empregar criptografia em todas as informações sensíveis, trafegar dados somente em túneis e usar tokens de autenticação de maneira extensiva nas trocas de informações com outros sistemas, dessa forma previne-se obtenção de dados por atacantes;

– Planejar em camadas de segurança, com o intuito de dificultar e/ou atrasar cada avanço do atacante em direção ao ativo valioso ao máximo. Conforme Oliveira (2012), é fundamental pensar sempre em como diminuir a área de ataque, minimizando ao máximo o impacto de uma sensibilidade caso ela seja explorável no futuro por uma brecha que venha a ser descoberta;

– Examinar corretamente as condições de segurança é fator decisivo para a sua correta implementação futura. Existem trabalhos inovadores que ajudam na tarefa de mapeamento automatizado destas condições vindas da linguagem natural, em que 80% deles são registrados rotineiramente nas RFPs e Documentos de Escopo de Projeto (PECLAT; RAMOS, 2014);

– Usar métodos automatizados de identificação de vulnerabilidades que alcançaram excelentes resultados em estudos comparativos, de acordo com Sagar et al. (2018).

5 PROPOSTA

A proposta deste trabalho é projetar uma arquitetura computacional eficiente para o sistema especialista responsável por processar e analisar diversas fontes de dados, tais como câmeras de vídeo, dados históricos de criminalidade, trânsito e iluminação e ao final gerar alertas para atuação imediata e um mapa da periculosidade em tempo real, resultando no aumento da eficiência operacional das forças de segurança da cidade inteligente.

Construir um sistema especialista exige uma análise criteriosa de todos os detalhes envolvidos, alguns desafios são apresentados, cujos principais são:

– Profusão de pessoas cadastradas: o número de pessoas procuradas em bases de conhecimento é enorme, facilmente chegando à casa dos milhões;

– Gravações simultâneas de imagens: uma metrópole pode ter milhares de câmeras registrando imagens em diversos lugares ao mesmo tempo com um fluxo intenso de pessoas;

– Controle da luminosidade: uma imagem registrada com alterações de iluminação e foco causa distorções e pode afetar de maneira significativa a precisão dos algoritmos de reconhecimento facial;

– Produzir alertas eficazes: uma abordagem eficiente, segura e veloz só é possível no caso de encontrar de maneira rápida a autoridade policial ou social mais próxima ao local repassando os dados de forma precisa;

– Proteção contra invasões: as imagens precisam necessariamente estar protegidas de acessos e manipulações externas não autorizadas, impedindo a modificação, inserção ou retirada de imagens ou dados do cadastro de uma pessoa foragida, portanto, essas imagens sempre serão sigilosas e sensíveis. A modificação ou desligamento de uma câmera de forma proposital caracteriza-se por ser outro objetivo criminoso para permitir uma ação sem ser identificada;

– Pose: de maneira geral, a instalação das câmeras ocorre em locais altos, o que possibilita uma ampla captura da região, no entanto, com isso o enquadramento do rosto fica impossibilitado, pois a imagem não é frontal, e na grande maioria dos casos a leitura dos algoritmos fica insuficiente quanto menor for a visão frontal dos rostos;

– Inclinação da cabeça: em geral, as pessoas não estão com a cabeça corretamente alinhada verticalmente, sendo necessária a aplicação de um pré-tratamento para alinhamento da imagem. É possível utilizar a posição das pupilas dos olhos como marcação de inclinação, conectando estes dois pontos e alinhando a imagem a partir desta reta (SAJJAD, 2019);

– Câmeras de resolução baixa: comumente são utilizadas câmeras com resoluções inferiores, o que diminui a precisão da captura dos pontos relevantes da face, devido à “pixelização” e interpolação nas imagens;

– Captura de muitas pessoas simultaneamente: quando há grande circulação de pessoas em um mesmo local, as câmeras podem registrar centenas de pessoas e identificar todas ao mesmo tempo, exigindo muito processamento paralelo do sistema;

– Disfarces: um foragido normalmente usa de disfarces para se esconder dificultando a identificação eficaz de alguns algoritmos de reconhecimento.

Estes são alguns dos desafios relevantes no processo de reconhecimento facial em uma cidade inteligente, uma vez que a captura destas imagens não acontece em um ambiente controlado.

Um dos principais problemas é a posição da face das pessoas no momento da solicitação do reconhecimento, pois em poucas situações consegue-se um registro de imagem ideal, frontal, com foco e nitidez e sem nenhum tipo de interferência externa de objetos que estejam ocultar parcialmente algum dos pontos relevantes do rosto.

Para aprimorar capturas inadequadas, são aplicadas técnicas computacionais que representam a imagem em 3D, o que permite rotacionar com melhor precisão as imagens para colocá-las na posição ideal para iniciar o processamento da análise.

A grande variação de luminosidade é outro aspecto muito relevante. Diversas fontes externas de luz podem fazer com que as imagens fiquem desfocadas ou parcialmente distorcidas, fatos que alteram a capacidade de identificação das características marcantes daquele rosto, ponto de partida do trabalho de reconhecimento.

A quantidade de imagens com boa resolução sendo capturadas ao mesmo tempo em centenas de milhares de câmeras ocasiona uma necessidade de transmissão de dados em redes de alta velocidade em diferentes pontos da cidade.

Dessa forma, para processar este grande volume de dados, o suporte computacional deve ser potente de maneira significativa e escalável a fim de atender à crescente demanda.

5.1 REQUISITOS FUNCIONAIS

O sistema deve ser projetado e implementado como um sistema de tempo real, pois os dados capturados geram informações seguindo as restrições temporais, ou seja, a definição de um intervalo de tempo entre as amostras consecutivas.

Implementar um sistema de tempo real não é uma tarefa simples, pois exige conhecimento profundo de diversos aspectos dos processos controlados e da Engenharia da Computação.

Um sistema de tempo real é um sistema computacional que deve reagir a um determinado estímulo oriundo de seu ambiente em um tempo máximo predefinido.

> [...] Estes sistemas são chamados de tempo real porque são projetados para executar tarefas de controle dependentes de tempo, devendo operar sob estritas condições de desempenho. Os sistemas operacionais embarcados que operam em tempo real são chamados de determinísticos, pois devem executar suas tarefas em um conhecido e previsível período (TAURION, 2005, p. 47).

O sistema utilizará cinco informações principais para a determinação da periculosidade, baseado nas informações disponíveis nas bases históricas de registros e na percepção de impacto da oportunidade para os criminosos:

1) Localização geográfica: mapeamento da latitude e longitude do local;

2) Horário: momento do dia no qual ocorreu o incidente relatado;

3) Iluminação: dados sobre a luminosidade imediata no local de interesse.

A iluminação é um dos maiores fatores que influenciam a oportunidade para um crime (Figura 4);

Figura 4 – Luminária Inteligente para postes públicos
Fonte: Philips (2014).

4) Trânsito: grande parte dos crimes ocorrem nas ruas, desta forma o trânsito tem significativa influência na oportunidade que os criminosos têm para praticar os ataques (Figura 5);

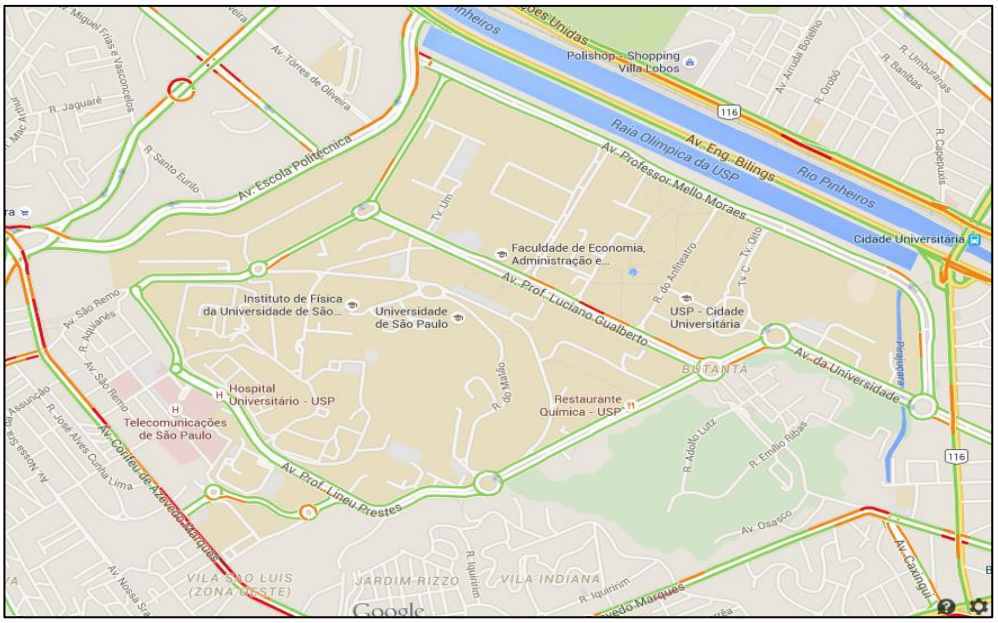

Figura 5 – Trânsito na Cidade Universitária Armando de Salles Oliveira
Fonte: Google Maps (2014).

5) Histórico: a quantidade e tipificação dos crimes já ocorridos em uma determinada localização são os fatores de maior influência na previsão da periculosidade. Porém, é importante observar que os crimes “migram” de lugar conforme exista o reposicionamento das forças de segurança.

Após a definição dos critérios importantes, inicia-se a construção das entradas fuzzy no software escolhido, sendo a Figura 6 o mapeamento da variável Iluminação, a Figura 7 o mapeamento do Trânsito e a Figura 8 a representação do dado de entrada Histórico de Criminalidade.

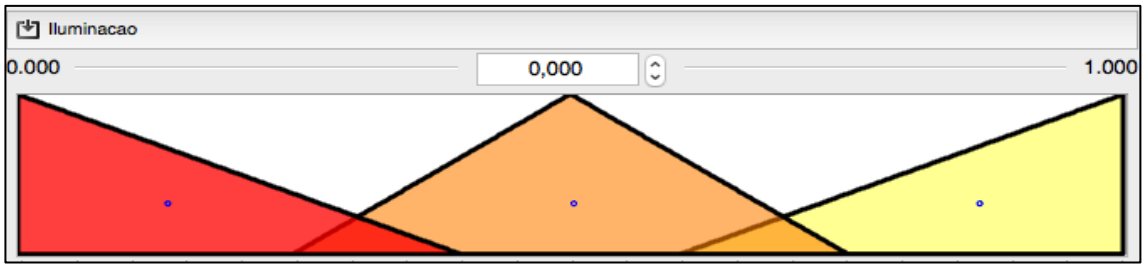

Figura 6 – Configuração da variável de Iluminação
Fonte: Elaboração própria através do Software FuzzyLite.

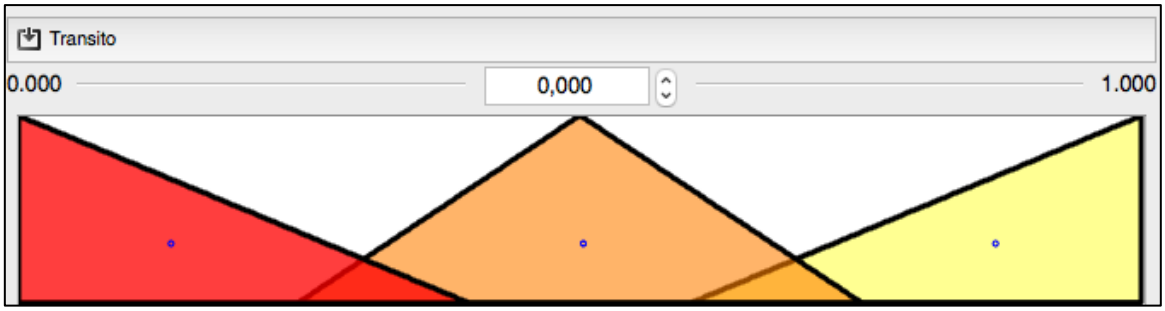

Figura 7 – Configuração da variável de entrada Trânsito
Fonte: Elaboração própria através do Software FuzzyLite.

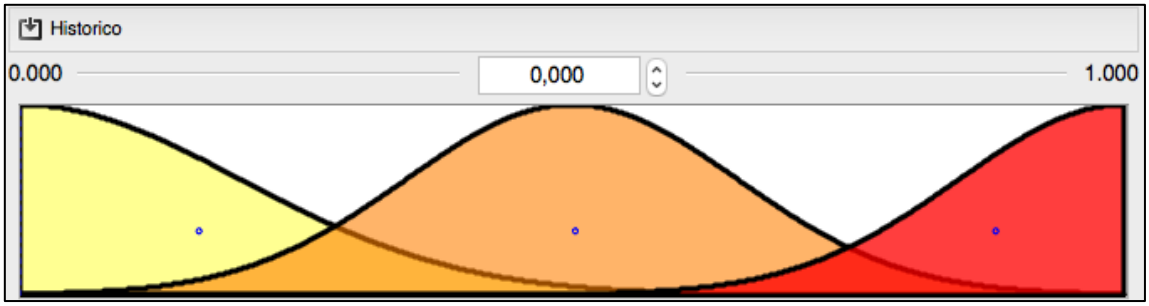

Figura 8 – Configuração da variável de Entrada Histórico de Criminalidade
Fonte: Elaboração própria através do Software FuzzyLite.

A Figura 9 apresenta um exemplo dos dados de iluminação, trânsito e histórico de criminalidade, após o processamento em batch, gerando o mapa visual de periculosidade de uma determinada área.

Figura 9 – Representação Visual do Mapa de Periculosidade
Fonte: Adaptado de Google Maps (2014).

O mapa de calor gerado poderia ser interpretado da seguinte forma:

– Pontos Verdes: o modelo considera de Periculosidade Baixa;

– Pontos Amarelos: o modelo considera áreas de Periculosidade Média, aconselha-se atenção nestes pontos, ou seja, uma probabilidade média de ocorrência de incidentes;

– Pontos Vermelhos: regiões com Periculosidade Alta, o modelo recomenda atuação imediata das forças de segurança para prevenir ou combater criminalidade nesta área.

O resultado final pretendido é inferir um mapa representativo dinâmico e atualizado em tempo real da periculosidade da cidade inteligente, similar ao exemplo hipotético abaixo, cuja imagem foi construída manualmente utilizando-se dados fictícios com o objetivo de demonstrar o resultado esperado ao final do processamento do algoritmo de predição (Figura 9).

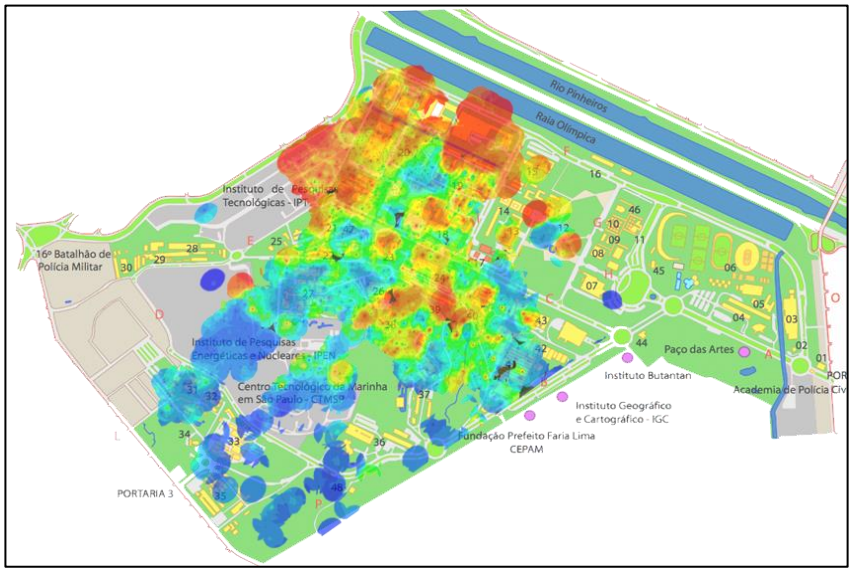

Figura 10 – Representação do Mapeamento de Calor Geográfico de Áreas
Fonte: Taste of Sustainability (2014); Stack Overflow (2014).

Pretende-se calcular o mapa de calor através da representação tridimensional dos eventos históricos e em tempo real recebidos, utilizando pesos calculados levando em consideração o tipo de crime, recorrência, horários e

também fórmulas de decaimento no tempo sobrepondo-o num mapa com as respectivas coordenadas geográficas.

Além disso, é preciso complementar os dados de ocorrências criminais com as informações sobre os eventos externos que possam mudar o mapa de oportunidades, como já citados anteriormente, como, por exemplo, problemas de iluminação e congestionamentos que entrarão como novos itens com pesos e fórmulas de decaimento específicas.

Esta abordagem dinâmica é necessária para que o sistema especialista se mantenha atualizado e que represente adequadamente a realidade, visto que a criminalidade está em constante evolução e migração de territórios.

A representação tridimensional dos riscos calculados poderá ser apresentada por um gráfico similar à Figura 10, sobreposto a um mapa da cidade, que estará posicionado no plano cartesiano “xy”, e as cotas “z” serão a estimativa matemática da periculosidade daquela coordenada geográfica em questão, ou seja, quanto mais alta a cota do ponto maior o seu risco estimado.

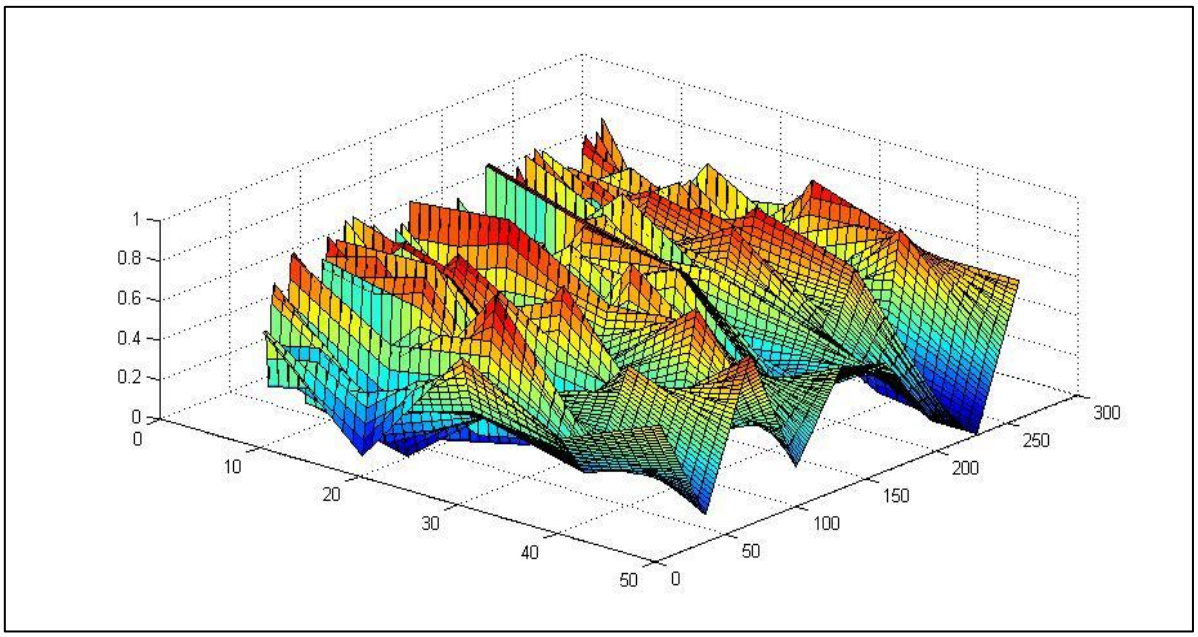

Figura 11 – Visualização 3D da representação matemática dos dados
Fonte: Stack Overflow (2014).

Desta forma, será possível seccionar o gráfico tridimensional em cortes de planos paralelos ao plano “xy” determinando classes de áreas, indo das mais perigosas até as mais seguras e atuar conforme manuais de conduta preestabelecidos em cada uma delas.

Para que se possa inferir estas informações é preciso lançar mão de algoritmos de análise preditiva baseados em dados históricos e também de dados adquiridos em tempo real, para prever e atuar em eventos que exijam intervenção policial.

Pode-se descrever, de forma simplificada, a arquitetura de um sistema de análise preditiva, como segue:

1) Aquisição: recebimento de informação em grande quantidade, segundo o conceito de Big Data do capítulo 5, de fontes distintas e com formatos diferentes entre si;

2) Normalização: tratamento dos dados, para simplificação e checagem se eles atendem aos requisitos necessários para entrar no banco de conhecimento pelos critérios definidos dos fatores importantes no capítulo 4;

3) Classificação (PAN et al., 2013): conversão do dado simples em informação classificada por tipo de evento e gravidade;

4) Clusterização (PAN et al., 2013; HART; ZANDBERGEN, 2012): aglutinação de itens por critérios de similaridade, como tipo, gravidade, localização física ou temporal dos eventos;

5) Ranqueamento (PAN et al., 2013): seleção dos clusters mais relevantes para buscar relações e informações relevantes;

6) Regressão multivariada (PAN et al., 2013): teste de correlações entre diversas possíveis combinações de causa e efeito;

7) Inferência: utilização de lógica fuzzy para determinação da melhor estratégia de policiamento baseado nas informações obtidas;

8) Apresentação de resultados: demonstração de forma simples e conclusiva dos dados inferidos pelo sistema especialista.

Com o correto mapeamento dessas áreas com periculosidade alta, será construído um algoritmo capaz de otimizar, em tempo real, o posicionamento das forças de segurança, deslocando-as de forma econômica e estrategicamente eficiente e monitorada para a sua posição ideal naquele instante, segundo o critério da minimização de áreas perigosas.

Em áreas de alta periculosidade, por exemplo, pode ser necessária a instalação de bases fixas com efetivos policiais constantes e em contrapartida reduzir rondas em áreas mais seguras da cidade sem efeito negativo.

A abordagem de transformação desse processo apresenta vantagens em relação ao processo atual baseado em decisões pessoais e empíricas, como, por exemplo:

1) Responder em tempo real a eventos importantes, como um assalto com reféns;

2) Tomar decisões adequadas e economicamente racionais, evitando deslocar recursos excessivos ao local onde não exista esta necessidade;

3) Reduzir a possibilidade de corrupção, visto que os policiais em patrulhamento ostensivo não saberão com antecedência o roteiro que será patrulhado;

4) Monitorar a eficiência e o cumprimento dos roteiros, em tempo real, indicando um desvio da rota planejada para que o responsável atue adequadamente, questionando a patrulha do motivo da mudança inesperada da rota predefinida;

5) Informar apropriadamente às patrulhas a velocidade que devem percorrer cada trecho e as indicações de periculosidade para que possam se preparar com antecedência a situações prováveis de risco.

A coleta de dados e a sua análise permitirão gerar três tipos inferências:

1) Diretas: constatar as relações de causa de um determinado evento, por exemplo, áreas inseguras, ou seja, com maior propensão de ocorrência de crimes;

2) Indiretas: relação de influência da ocorrência de um evento em outro, por exemplo, aumento de incidentes de segurança relacionados a problemas de iluminação deficiente em pontos da cidade;

3) Complexas: combinação de situações que aumentarão a probabilidade de ocorrência de eventos, como, por exemplo, previsão de chuva forte implicará em alagamentos pontuais, que por consequência gerarão trânsito lento em pontos específicos, situação essa que gera um risco maior de incidentes de segurança para roubos a motoristas.

É possível perceber que obter estas informações permitirá aprimorar a cidade e assim torná-la mais segura (SHEKHAR et al., 2012; GREENGARD, 2012; IBM, 2014) e agradável para todos seus habitantes.

O sistema especialista poderá ser incorporado como um módulo do Sistema Integrado de Gestão da Infraestrutura Urbana (SIGINURB), que por sua vez tem por objetivo tornar a Cidade Universitária Armando de Salles Oliveira (CUASO), em São Paulo, mais inteligente através da integração dos processos urbanos, melhorando os controles existentes e gerando a coordenação necessária das ações para uma Gestão Integrada (Figura 12).

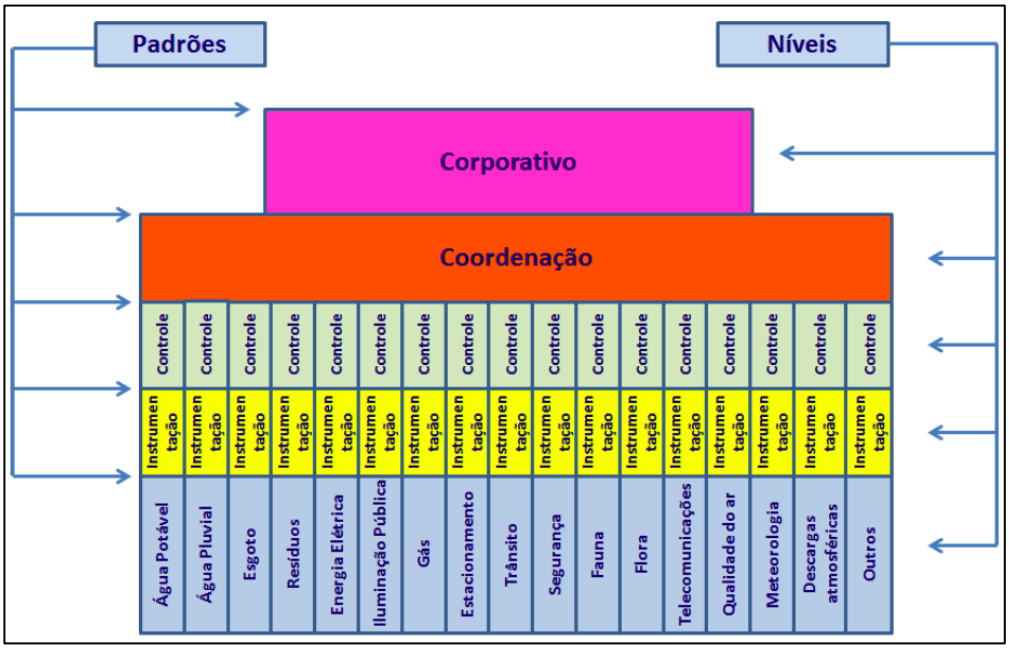

Figura 12 – Mapeamento da gestão integrada
Fonte: Martini (2013).

Existem diversas outras iniciativas acontecendo mundialmente. Pode-se citar notoriamente o Rio de Janeiro (ROCHE et al., 2012; IBM, 2014), onde foi implantado recentemente um dos mais modernos centros de operações urbanas, que engloba 32 agências de serviço público integradas, trabalhando juntas. Em Memphis e Miami-Dade (EUA) (IBM, 2014), a polícia tem utilizado extensivamente este tipo de análise para redução da criminalidade.

5.2 REQUISITOS NÃO FUNCIONAIS

– Alta disponibilidade: construir um sistema especialista que sempre esteja ativo para processar as informações recebidas, trabalhando com redundância de componentes e sem pontos únicos de falha;

– Confiabilidade: utilizar componentes com alta qualidade, ou seja, alto tempo médio entre falhas, e níveis adequados de robustez definidos pelas normas militares para trabalhar em situações de uso contínuo e ambiente hostil, externo e não controlado;

– Detecção de falhas: ser capaz de identificar um componente com problemas, limitar sua atuação e sinalizar para conserto, pelo responsável, inclusive com a utilização do tempo de atendimento através do acordo do nível de serviço (SLA – Service Level Agreement, em inglês ou Acordo de Nível de Serviço) adequados à criticidade destes equipamentos para esta correção, se possível utilizar mecanismos automatizados para se recuperar autonomamente desta falha;

– Determinismo: ser capaz de calcular o mapa de periculosidade dentro de intervalos predefinidos para que os responsáveis possam tomar decisões baseadas nas informações atualizadas em tempo real e confiáveis;

– Comunicação segura: por se tratar de um sistema de coleta de informações distribuído, a comunicação entre seus componentes deve ser segura, sigilosa e confiável;

– Documentação: manter todo o material utilizado na especificação e implementação da pesquisa agrupado e organizado para que ele sirva de base para uma evolução segura do desenvolvimento do sistema especialista ao longo da sua vida útil;

– Software: é preciso levar em consideração principalmente os seguintes pontos:

> – Sistema operacional: o sistema operacional deve ser eficiente, preemptivo, seguro e capaz de permitir um controle sobre os recursos alocados, coordenação e escalação entre os processos e também o uso de interrupções para criar um sistema previsível;
>
> – Tolerância a falhas: deve ser capaz de funcionar com redundância e, quando possível, detectar e corrigir as falhas em seus componentes;

– Linguagens de programação: deve ser capaz de trabalhar diretamente com os recursos da máquina para que possa reservar e utilizar os elementos necessários no momento em que forem solicitados, tais quais memória, processamento, I/O, rede, etc.;

– Processamentos síncronos e assíncronos: gerenciar diferentes tipos de eventos para construção de uma solução robusta e sem variações ao longo do tempo.

– Hardware: os equipamentos responsáveis pela aquisição e processamento de dados de supervisão, controle, movimentação e armazenamento de dados, interface com o mundo externo, comunicação de um sistema de tempo real precisam guardar as seguintes características:

– Velocidade de resposta: o processamento destas informações deve ser feito de forma a atender a SLA de atualização dos dados;

– Confiabilidade: utilização de componentes de reconhecida qualidade, redundância, cópias de segurança das informações armazenadas em locais seguros, detecção e correção de falhas;

– Transferência de dados: ser capaz de movimentar e armazenar grandes quantidades de dados eficientemente;

– Robustez: ser capaz de trabalhar sem alterações em ambientes não controlados e muitas vezes hostis, com temperaturas, umidade, poeira, trepidação, interferências eletromagnéticas, etc.;

– Suporte: o fabricante deve possuir um nível adequado de qualidade de pós-venda e suporte medido pela SLA, a fim de manter em funcionamento a operação contínua ao longo do tempo;

– Paralelismo: o sistema irá fazer uma extensa quantidade de cálculos matemáticos para inferir o gráfico de periculosidade, portanto, poder utilizar recursos em paralelo é importante para que se possa reduzir o tempo total de resposta.

5.3 VIÉS

Um dos maiores desafios encontrados atualmente é a construção de sistema de reconhecimento de imagem que não possua nenhum tipo de viés, ou seja, uma propensão para reforço de um comportamento.

Caso um sistema contenha um viés, ele pode repetir um comportamento humano indesejável, principalmente o preconceito racial e o machismo.

Já houve casos largamente divulgados sobre uma diferença significativa de precisão para reconhecer rostos de mulheres negras quando comparadas ao reconhecimento de rostos masculinos de pessoas brancas (LOHR, 2018).

Outro caso são sistemas de recrutamento de currículos para vagas de emprego, nos quais são reforçados padrões de recomendação de contratação de homens em detrimento das mulheres em empresas de tecnologia, como reportado em um caso recente da Amazon (DASTIN, 2018).

Estes casos acontecem com uma certa frequência, principalmente por terem sido treinados de forma desbalanceadas, sem a utilização dos exemplos corretos de demonstração das características exatas de qualidade de um candidato ou mesmo de um rosto em diferentes situações.

Muitas destas imagens possuem uma ou mais informações, por exemplo, é possível encontrar bases de dados de animais em diversas situações, tais como ambientes internos das casas ou na natureza.

Então, se, por exemplo, ao se treinar uma rede neural com muitas fotos de gatos em um ambiente de um apartamento e, por outro lado, se utilizar diversos exemplos de cachorros passeando na rua ou parques, quando o sistema for questionado para classificar uma imagem de um gato em uma árvore, certamente sua precisão não será a ideal, provavelmente errará a sua classificação.

Isto se deve à forma como as redes neurais funcionam intrinsicamente, quando elas recebem dezenas, centenas ou milhares de exemplos de uma determinada classe de objetos suas estruturas buscam padrões entre elas para

que possam buscar estes mesmos padrões quando forem solicitadas para analisar outros exemplos.

Então, de uma forma simplista, no exemplo dos gatos de apartamento, é possível que a rede neural determine que um fator relevante seja a presença de paredes, ou de móveis, ou até mesmo a ausência de plantas como sendo um marcador para alta probabilidade de uma imagem conter um gato.

Sabe-se que gatos saem menos para passear com seus donos do que cachorros, porém ao utilizar este fato como um marcador de alta probabilidade, insere-se no sistema um certo tipo de preconceito, ou seja, se é um animal que esteja ao ar livre não será um gato, o que obviamente sabe-se que é verdade.

Com este exemplo é possível perceber que treinar uma rede neural de forma incorreta pode incidentalmente ensiná-la a repetir um comportamento preconceituoso ou discriminatório que exista consciente ou inconscientemente dentre aqueles responsáveis por esta tarefa de extrema importância.

Neste caso, a melhor forma de resolver, ou pelo menos minimizar, os eventos deste desbalanceamento é mostrar para rede neural outros exemplos que a ajudem a aprimorar o seu aprendizado, realmente concentrando sua análise nos elementos comuns desejáveis, tais como as características físicas dos gatos *versus* cachorros, e não no ambiente nos quais eles normalmente são fotografados, para que esta última característica não passe a se tornar uma exigência para o processo de classificação.

Desta forma é necessário conhecer a fundo as características deste tipo de algoritmos para que se possa extrair os melhores resultados, seja escolhendo corretamente qual classe de rede neural utilizar e como escolher os exemplos de treinamento positivo e negativo.

No processo de escolher os exemplos é importante questionar os próprios preconceitos e principalmente trabalhar em times multidisciplinares em que se consiga reunir pessoas de diferentes opiniões que componham uma perspectiva mais ampla e abrangente de mundo.

5.4 EQUIPAMENTOS

A escolha dos equipamentos a serem utilizados em campo pelos responsáveis da segurança pública é uma tarefa extremamente importante para garantir o funcionamento ao longo do tempo.

Alguns fatores são importantes e devem ser levados em consideração no momento da escolha:

1) Segurança: deve ser um equipamento com defesas físicas e lógicas para evitar invasões que permitam manipular as informações por pessoas não autorizadas. Normalmente é necessário escolher um equipamento que não permita a desmontagem física sem que ele seja automaticamente desligado e um sistema operacional moderno e seguro contra as invasões cibernéticas;

2) Robustez: o hardware deverá ser construído e testado para operar em condições de adversidades climáticas, tais como altas temperaturas dentro de um veículo, chuva, frio, umidade e até eventuais pequenos incidentes como quedas precisam ser levados em consideração na escolha do equipamento;

3) Peso: a mobilidade é um fator que deve ser levado em consideração, para permitir que o equipamento acompanhe o responsável pela segurança em suas missões, não se tornando um entrave para o seu desempenho.

Podem ser listados alguns tipos de equipamentos que sejam capazes de ser utilizados para enviar e receber informações para o sistema de monitoramento urbano:

1) Celulares e tablets: podem consultar informações em tempo real e submeter imagens de pessoas para uma busca no banco de dados de identificação;

2) Relógios smart: devido ao seu peso e facilidade de uso podem ser empregados para o recebimento de informações e alertas;

3) Câmeras acopladas ao corpo: permitem a captura de imagens em locais inacessíveis para câmeras fixas, como por exemplo, um policial caminhar em uma calçada ou em meio a uma manifestação buscando identificar pessoas procuradas;

4) Óculos de realidade aumentada: permitem mostrar ao oficial responsável de forma simples e direta uma sinalização visual de qual é a pessoa que deverá ser interceptada para averiguação pelos órgãos responsáveis policiais ou sociais, a depender do tipo de alerta ativado.

Com a popularização destes tipos de equipamentos é esperado que seus custos sejam significativamente reduzidos e permitam um uso massivo entre todos os envolvidos na segurança da cidade.

5.5 SINTETIZAÇÃO DE EXEMPLOS PARA TREINAMENTO

Uma das técnicas que pode ser empregada para minimizar o bias em redes neurais para aprendizado supervisionado é a geração automática de exemplos para eliminação de elementos não relevantes.

Por exemplo, quanto à percepção do impacto do ambiente externo no caso de classificação de imagens de gatos e cachorros, é possível a geração de centenas de imagens de situações com um mesmo gato com diferentes imagens de fundo, recortando a imagem original, deixando somente o contorno do gato e sobrepondo esta imagem em diferentes planos de imagens de natureza e ambientes urbanos.

O mesmo tipo de ação pode ser utilizado para tonalização de pele, treinando o algoritmo com todas as pessoas simulando diferentes tons de pele por colorização por algoritmo, desta forma um mesmo rosto seria ensinado para uma rede em dezenas de tons de pele e ele perceberia que isto não é relevante, somente os traços de contorno, pontos específicos do rosto, medidas relativas

entre eles são as informações que de fato definem aquele objeto, que no caso seria o rosto da pessoa que está sendo ensinado.

No caso de discriminação entre mulheres e homens em currículos, pode-se, de forma simplista, somente retirar a informação sobre o gênero da pessoa do currículo, porém é conhecido que os computadores conseguem determinar com boa precisão textos escritos por homens e mulheres, pela utilização de estruturas gramaticais e padrões de escrita diferentes.

Sendo assim, a forma mais eficiente é o treinamento de um currículo em dois formatos, duplicando sua versão, sobrepondo as características do sexo oposto, de uma forma simplista, reescrevendo-o como o computador pensaria que ele teria sido se fosse o outro gênero quem o fizesse.

5.6 GPUs (GRAPHICS PROCESSING UNIT)

As GPUs surgiram para processamento mais eficiente dos gráficos nos computadores, assim como o próprio nome diz. São chips que foram construídos com o foco em fazer cálculos necessários para renderização de objetos visuais mais eficientemente do que as CPUs tradicionais CISC (Complex Instruction Set Computing) e RISC (Reduced Instruction Set Computing) fariam.

Para que uma imagem seja representada corretamente através de um formato de fotografia ou de vídeo, é necessário executar uma série de cálculos para posicionar corretamente as cores de cada um dos pixels da tela.

Se estas tarefas complexas ficassem somente a cargo da CPU, esta não teria capacidade de processamento para executar outras funções necessárias para manter o restante do computador funcionando corretamente, tais como gestão de memória, acesso ao disco, interface homem-máquina, acesso à rede, etc.

Porém, os pesquisadores de Inteligência Artificial rapidamente perceberam que poderiam se aproveitar deste grande poder computacional e executar tarefas matematicamente similares nestes chips, mesmo não se tratando do processamento de imagens.

A utilização de GPUs é uma forma eficiente de acelerar o processamento das redes neurais, pois este tipo de chip consegue fazer cálculos matemáticos de ponto flutuante em uma velocidade muito superior às CPUs.

As GPUs modernas possuem centenas e em alguns casos até milhares de núcleos (cores) de processamento, o que permite um nível de paralelismo significativamente mais alto do que aquele que poderia ser obtido nas CPUs para cálculos paralelizáveis, no caso de redes neurais é muito útil em multiplicação de matrizes, visto que este outro tipo de chip normalmente possui menos do que uma dezena de núcleos.

Outra qualidade é que a GPU possui uma largura de banda muito maior para acessar a memória do computador, o que permite movimentar mais eficientemente uma quantidade maior de dados evitando que este processo possa se tornar um gargalo da performance.

A desvantagem da GPU frente à CPU é a quantidade de memória interna que na maioria dos casos chega a ser milhares de vezes menor. Porém, é possível contornar este problema utilizando a estratégia de dividir o processamento em pequenas parcelas e as executar paralelamente, explorando sua incomparável capacidade de alocar até milhares de unidades de processamento simultaneamente para execução de tarefas e seu rápido acesso à memória principal para buscar os dados de entrada e devolver as saídas já processadas.

Somente nos últimos anos se intensificou a pesquisa em aprimorar os frameworks responsáveis por processar softwares de inteligência artificial a fazer uso de forma menos complexa destes chips.

Alguns frameworks mais conhecidos de inteligência artificial fazem esta tarefa até de forma transparente, otimizando o código objeto para se beneficiar eficientemente da escolha de onde processar cada uma das instruções, seja ela na CPU ou GPU do computador, quando ambos estiverem disponíveis.

Com a popularização das nuvens públicas, com facilidade e custos relativamente acessíveis, já é possível alocar recursos em um cluster de GPUs para se fazer o treinamento das redes neurais de forma rápida e eficiente.

Estas empresas de nuvens computacionais permitem contratar a alocação destes equipamentos altamente eficientes, cobrando de forma fracionada por segundos. Desta maneira, é possível programar os algoritmos em máquinas comuns e com hardwares de baixo custo e quando for preciso de fato treinar a rede neural para que ela faça todo o processo de cálculo dos pesos dos perceptrons para convergir para um aproximação matemático de alta precisão, é

possível alocar estes recursos pelo tempo necessário, sejam alguns segundos, horas, dias, etc., e receber a cobrança somente por este tempo e não como anteriormente, quando era necessária a compra de equipamentos extremamente caros e de uso de poucas horas por mês.

O uso desta estratégia de combinar o uso de GPUs com a facilidade de alocá-las sob demanda e pagando um valor relativamente mais barato permitiu um aumento do uso de redes neurais em áreas novas.

O aumento da precisão é um fator que depende de ajustes nos pesos e hyper parâmetros da rede neural e também dos exemplos e contraexemplos utilizados para treinar a rede, sendo que cada mudança nestes itens exige um retreinamento, portanto, a eficiência no processo de treinamento impacta diretamente no resultado final entregue pela rede neural.

5.7 INTEGRAÇÃO COM FONTES EXTERNAS E PARTICULARES DE IMAGENS

O modo de aumentar a cobertura geográfica da cidade pelo sistema é expandir o número de câmeras instaladas.

Porém, sabe-se que estes equipamentos podem ser caros e seu funcionamento igualmente custoso, quando se leva em consideração os valores de manutenção e transmissão de dados online para sistemas externos de monitoramento ou backup.

O modo mais eficiente para o poder público aumentar sua cobertura é permitir a integração de fontes externas particulares de capturas de imagens, tais como câmeras externas de condomínios, empresas, concessionárias públicas ou mesmo residências.

O sistema ganharia automaticamente uma capacidade maior de monitorar áreas onde não tinha a devida visibilidade, por não ter os equipamentos e aqueles que permitem enviar suas imagens para serem acopladas ao sistema tendem a se tornar mais seguras, visto que no caso de detecção de uma situação de emergência será gerado um alerta automático de forma mais eficiente para os responsáveis mais próximos atuarem prontamente.

Já é bastante comum que as investigações policiais solicitem acesso a estas câmeras, porém este processo acontece muito após ao fato ocorrido. Fazendo-se uso em tempo real destas imagens é possível buscar um efeito

preventivo de possíveis atividades criminosas, trazendo um benefício claro e real para a sociedade.

Desta forma é possível estruturar um mecanismo de ganho mútuo entre as partes, que buscam ao final um objetivo comum, tornar a cidade mais segura para todos.

Para que este processo tenha uma adoção significativa é preciso que o cidadão que tenha a imagem para disponibilizar para o sistema possa fazê-lo de forma simples e rápida, devendo levar em consideração os seguintes aspectos:

1) Compatibilidade na transmissão das imagens: é preciso suportar os principais protocolos-padrão de formatos de imagem e vídeo;

2) Sistema eficiente de recepção de imagens: o volume de dados recebidos será significativamente maior do que somente as câmeras públicas;

3) Custo reduzido ou subsidiado para a transmissão destas imagens: o valor das transferências das imagens para os servidores públicos deve ser gratuito ou bastante reduzido levando-se em consideração a função social provida por estas imagens.

5.8 NECESSIDADE DE TREINAMENTO

Como toda nova técnica a ser incorporada pelos gestores da cidade, o sistema proposto traz uma série de novidades tecnológicas que precisarão ter seu conhecimento disseminado entre seus usuários.

A qualidade do treinamento é um fator crítico para o sucesso de um sistema tecnológico, pelos seguintes fatores:

1) Diminui a resistência à novidade: grande parte dos seres humanos possui uma resistência, muitas vezes inconsciente, a mudanças. É preciso diminuir esta resistência dentre os usuários do sistema para que se sintam à vontade para buscar aprender corretamente sobre seu funcionamento;

2) Utilização do sistema: para ser possível extrair o benefício máximo de todas as funcionalidades implementadas é preciso conhecer todas as capacidades que o sistema possui e como ele poderá ser utilizado;

3) Suporte: dúvidas e problemas podem acontecer durante o uso diário do sistema, quando os responsáveis se depararem com estas situações é preciso saber claramente onde procurar as informações necessárias e quem deverá ser acionado no caso de não ser possível resolver o problema somente com o manual de consulta disponível;

4) Melhorias: os usuários do sistema normalmente são uma ótima fonte de ideias de possíveis pontos de melhorias para otimização de uso do sistema. Criar e manter este canal de informações fluído, explicando a forma de utilização é de extrema importância para gerar um benefício crescente para a cidade inteligente.

5.9 LÓGICA FUZZY NO MAPEAMENTO PREDITIVO DINÂMICO

Conforme o Quadro 1, fez-se o mapeamento das regras fuzzy para construção da máquina de inferência e é apresentado o mapa de riscos, com o resultado em Lógica Fuzzy, que deve ser exposto no caso das variáveis primárias apresentarem os valores possíveis de serem observados de forma combinada.

Por exemplo, se o Trânsito estiver qualificado como “Intenso” e a Iluminação como “Ruim” em um local de Incidência de Crimes com Histórico “Baixa Incidência”, a Periculosidade será declarada como “Atenção”.

	Baixa Incidência de Crimes		
	Trânsito Intenso	Trânsito Normal	Trânsito Vazio
Iluminação Boa	Baixa	Baixa	Baixa
Iluminação Regular	Baixa	Baixa	Baixa
Iluminação Ruim	Atenção	Baixa	Atenção
	Média Incidência de Crimes		
	Trânsito Intenso	Trânsito Normal	Trânsito Vazio
Iluminação Boa	Atenção	Baixa	Baixa
Iluminação Regular	Atenção	Baixa	Baixa
Iluminação Ruim	Alta	Baixa	Atenção
	Alta Incidência de Crimes		
	Trânsito Intenso	Trânsito Normal	Trânsito Vazio
Iluminação Boa	Atenção	Baixa	Atenção
Iluminação Regular	Alta	Baixa	Atenção
Iluminação Ruim	Alta	Atenção	Alta

Quadro 1 – Configuração das regras Fuzzy de inferências
Fonte: Elaboração própria.

Para melhor entendimento, as regras de referência em Lógica Fuzzy foram disponibilizadas no Apêndice A.

A Figura 13 apresenta o processo para representar a variável periculosidade fuzzy de saída.

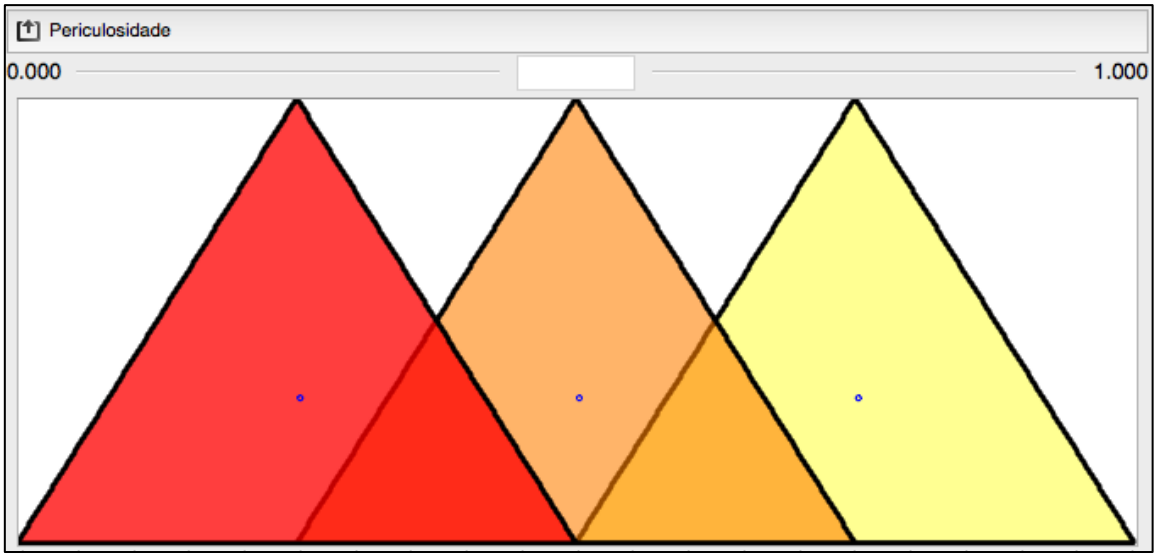

Figura 13 – Configuração da variável Fuzzy de saída periculosidade
Fonte: Elaboração própria através do Software FuzzyLite.

Para exemplificar a aplicabilidade do algoritmo do sistema especialista em uma situação hipotética, foi selecionada a cidade universitária Armando de Salles Oliveira como ponto central para análise, mapeando 500 pontos próximos aleatoriamente.

Conforme afirmado, como ainda não existe integração com as bases reais de dados públicos, para cada um destes 500 pontos mapeados foram gerados os dados hipotéticos para as três variáveis (iluminação, trânsito e histórico de criminalidade) aleatoriamente para se poder validar o modelo matemático.

Para melhor entendimento do funcionamento do Modelo Matemático de cálculo de periculosidade em Lógica Fuzzy foi disponibilizado no Apêndice B o código fonte Java.

Este algoritmo gera os resultados defuzzyficados, ou seja, convertidos para sua interpretação textual (Periculosidade: Alta, Baixa ou Atenção) para cada tripla de valores de entrada e desta forma pode-se comparar com os dados anteriormente disponíveis e descobrir qual é o valor esperado da periculosidade, por um especialista, naquele local, validando-se assim o funcionamento do modelo proposto.

6 ARQUITETURA DO SISTEMA

O sistema computacional de reconhecimento facial para monitoramento de uma cidade inteligente precisa ser projetado levando-se em consideração alguns detalhes para que funcione corretamente:

1) Streamming de vídeos: deve ser capaz de receber uma grande quantidade de vídeos contínuos e simultaneamente direcioná-los para os algoritmos responsáveis pela detecção dos rostos nas imagens;

2) Fila de processamento de detecção de imagens: as imagens a serem processadas devem ser armazenadas em uma fila de dados para permitir que sejam processadas assincronamente, acionando os algoritmos de detecção de rostos e eventos como, por exemplo, incêndio e pessoas caídas;

3) Algoritmo de detecção de rostos: este algoritmo é o responsável por analisar uma imagem e identificar se ela contém rostos, delimitá-los utilizando bounding box e recortar estes objetos identificados para enviá-los para a próxima fila, seja ela a de correção de imagem parcialmente identificada ou diretamente para o reconhecimento facial;

4) Fila de processamento de correção de imagens: responsável por armazenar e paralelizar as chamadas para os diferentes algoritmos de correção de imagem: pose, inclinação da cabeça ou sombra;

5) Correção de imagem: cada um dos algoritmos desenvolvidos tem uma atribuição claramente definida de qual é a correção que executará e assim que esta é completada, a imagem é encaminhada para a fila de reconhecimento facial;

6) Reconhecimento facial: neste processo obtém-se as características de um determinado rosto e são feitas as devidas buscas no banco de dados previamente construído para encontrar aquele que tenha a maior

similaridade. Caso nenhum deles esteja dentro da distância mínima a ser considerada, é declarado como sendo um novo rosto e este deve então ser armazenado expandindo um pouco mais a base de dados previamente existente;

7) Armazenamento do rosto reconhecido: quando um novo rosto é identificado é preciso que suas características sejam extraídas e ele passe a compor o banco de dados de informações para posteriores consultas. Este processo deve ser feito de forma muito eficiente para que o banco de dados não se torne excessivamente grande e, principalmente, mantenha-se rápido para consultas em tempo real;

8) Geração de alertas: sempre que uma situação relevante é identificada é preciso gerar um alerta para que um funcionário público, seja ele policial ou um agente social, possa atuar para resolver a emergência identificada;

9) Localização do agente mais próximo: assim que um alerta é gerado em uma câmera é preciso encontrar quais são os responsáveis mais próximos para que possam atuar rapidamente naquele evento identificado. Este processo exige manter atualizado em tempo real a localização de todos os agentes e ser capaz de calcular rapidamente a distância entre as pessoas e os locais que precisam de presença imediata;

10) Log: todas as atividades, identificações e alertas ficam armazenados em um log no sistema para permitir auditoria sobre este e aprimoramentos em sua precisão;

11) Os eventos ocorridos servirão como dados de entrada para o algoritmo de predição que calculará a probabilidade de ocorrência de um novo evento em cada um dos pontos da cidade inteligente, gerando assim o mapa de periculosidade;

12) Backup: armazenamento das imagens recebidas para consulta posterior. Caso elas tenham alguma marcação de um evento importante,

por exemplo, reconhecimento do rosto de uma pessoa procurada, esta imagem se mantém armazenada por tempo indeterminado. Caso não exista nenhuma sinalização, ela ficará arquivada por um período determinado, normalmente entre 30 e 90 dias.

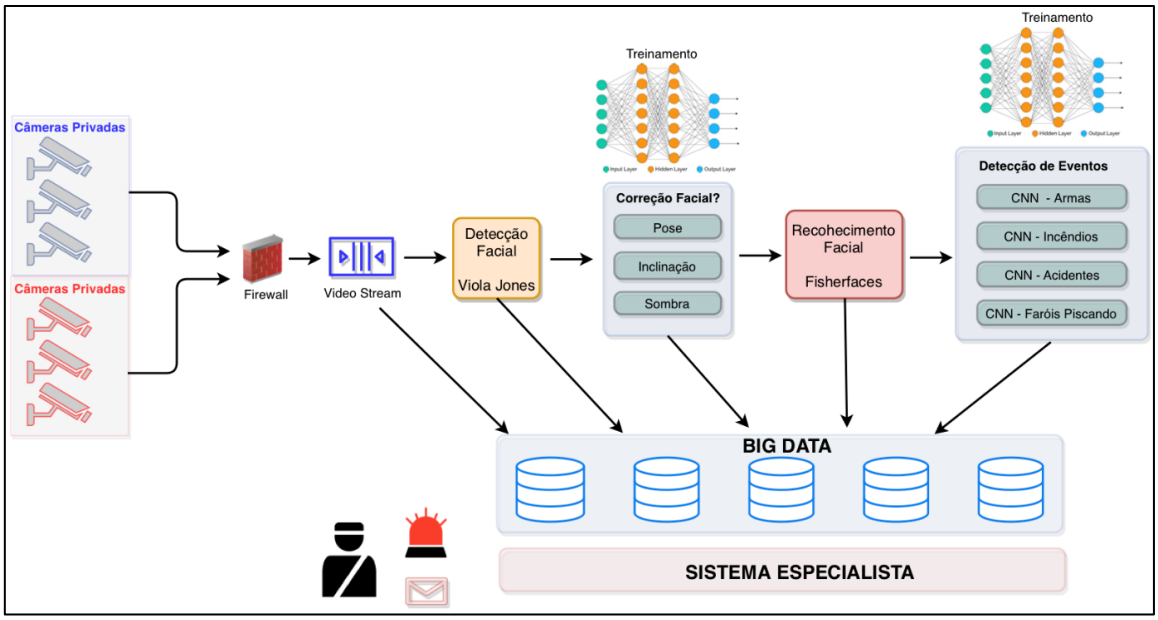

Figura 14 – Arquitetura do Sistema de Reconhecimento Facial
Fonte: Elaboração própria.

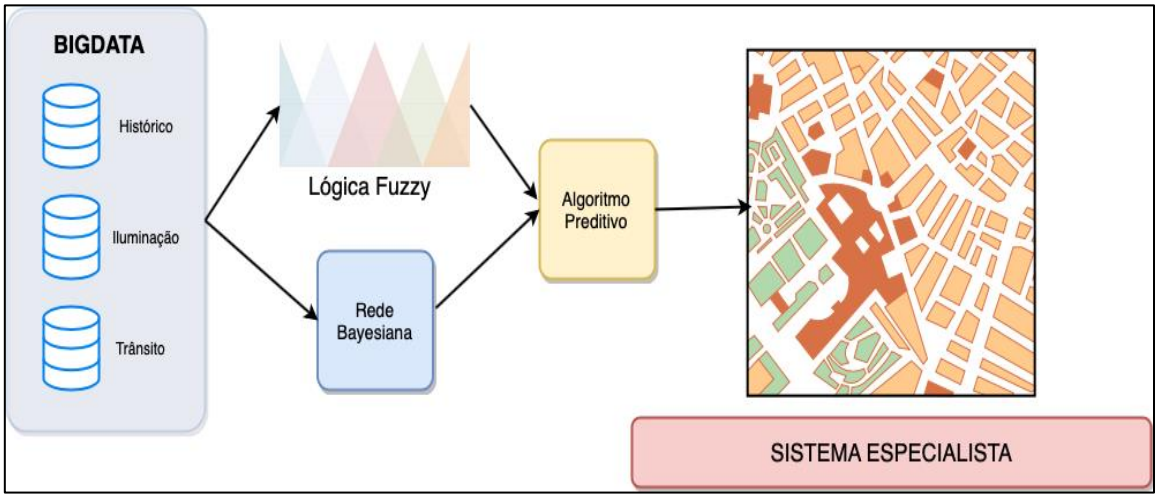

Figura 15 – Arquitetura do Sistema de Predição de Periculosidade
Fonte: Elaboração própria.

A arquitetura computacional proposta acima capacita o sistema especialista para atender cada um dos diversos e exigentes requisitos funcionais e não funcionais necessários para prover o alto nível de serviço exigido, entregando resultados precisos e em tempo real para o suporte à decisão dos responsáveis pela segurança da cidade inteligente.

Esta arquitetura foi projetada levando em consideração ser eficiente economicamente, utilizando os recursos públicos custeados pela sociedade de forma racional e otimizada.

7 TRABALHOS FUTUROS

No futuro é possível expandir a capacidade de compreensão de contexto utilizando Machine Learning para entender situações socialmente mais complexas, tais como:

– Deficiência de transporte público: baseado na contagem e tempo de permanência das pessoas nos pontos de ônibus e terminais;

– Necessidade de atividades escolares complementares: análise da quantidade de crianças fora de casa em horários não escolares, podendo estimular o poder público a criar iniciativas para proteger e evitar espaço para o assédio para criminalidade;

– Obras públicas: monitoramento de eventos na cidade, como um vazamento de água, esgoto, gás, etc.;

– Acompanhamento dos servidores públicos: monitorar o tempo de atendimento dos serviços solicitados, se existe morosidade excessiva nos deslocamentos e retornos aos seus postos;

– Proteção ambiental: acompanhar atividades que possam significar impactos ambientais, como atividades de descarte de lixo e entulhos em locais inapropriados, como terrenos, rios, mananciais.

7.1 ASSINATURAS SONORAS

Nos últimos anos as pesquisas utilizando redes neurais para reconhecimento de sons, principalmente vozes, têm avançado drasticamente.

Atualmente já é possível comprar equipamentos que funcionam como assistentes pessoais, ouvindo e interagindo com as pessoas de forma contínua nas residências ou escritórios. Estes equipamentos conseguem extrair informações do ambiente no qual estão inseridos para compreender o contexto da pergunta que está sendo feita e responder adequadamente, até mesmo a

forma como deve se responder a um estímulo, desde o volume, tom de voz, sotaque ou uso de um vocabulário mais formal ou popular.

As cidades inteligentes geram muitos sons, e estes podem também ser utilizados para extrair informações sobre o ambiente onde são capturados.

É possível ouvir vozes conversando, porém seria muito complicado obter informações relevantes sobre o que de fato é falado pelas pessoas, pois existem algumas situações diferentes, visto que algumas conversam entre um grupo totalmente presente naquela cena, como, por exemplo, um casal ou uma família e existem casos onde a conversa ocorre parcialmente na cena, como uma pessoa falando ao telefone celular.

Neste caso o importante é a captura de alguns padrões sonoros conhecidos ou uma assinatura sonora de alguns tipos de eventos que possam gerar alertas diretamente, como, por exemplo:

– Explosão;

– Tiros;

– Estilhaço de vidros;

– Colisão de automóveis;

– Gritos;

– Sirenes;

– Alarmes de invasão de imóveis.

Outra característica sonora que pode ser utilizada de forma muito eficiente é a localização do evento baseado em triangulação.

Segundo a Física, o som se propaga com velocidade uniforme em todas as direções em um determinado meio, no caso, o ar. Sendo a velocidade do som no ar conhecida, aplica-se o cálculo de ajuste para levar em consideração a

intensidade e direção do vento, e então é possível estimar a distância do evento gerador ao receptor em linha reta pelo tempo que o som demorou para atingi-lo.

Desta forma, tendo pelo menos três fontes de captura posicionadas adequadamente sobre um determinado plano, é possível estimar com uma boa precisão a localização do evento.

Se as câmeras também forem capazes de capturar o som ambiente, é possível processar este sinal em busca das assinaturas sonoras classificadas como importantes.

Quando elas são encontradas em diferentes equipamentos, calcula-se a diferença de tempos entre eles e desenham-se raios da distância estimada sobre um mapa que tenha a posição geográfica destes microfones.

Onde houver a intersecção destes círculos será o ponto estimado da ocorrência do evento sonoro reconhecido.

Podem existir algumas imprecisões neste método em razão de ecos gerados pelos objetos que possam refletir os sons em direções e tonalidades diferentes, tais como paredes de prédios, fachadas de vidro, etc.

Desta forma é possível aumentar ainda mais a capacidade de extração de informações em uma cidade inteligente, mesmo sem ter as imagens de todas as ruas e imóveis.

Com um sistema como este é possível a identificação em tempo real de uma explosão de um botijão de gás em um prédio residencial ou caixa eletrônico; pode-se saber de um evento de um disparo de arma de fogo em uma rua ou dentro de um imóvel mesmo que não exista imagem sobre este local.

Existem microfones de alta sensibilidade que podem ser colocados no alto de locais estrategicamente posicionados, de média altitude que possam capturar sons de alguns quilômetros quadrados aumentando ainda mais a segurança pela geração rápida de chamados e alertas.

7.2 DRONES

Conjuntamente com a estratégia da utilização de câmeras e microfones para detecção de eventos é possível a utilização de drones para complementar a camada de monitoramento quando não houver uma câmera posicionada no ângulo desejado.

Por exemplo, quando for detectado um evento de explosão, um drone pode ser deslocado de forma automática para as proximidades do local e começar a transmitir a imagem para um centro de controle.

Nestes casos de deslocamento automático é preciso levar em consideração alguns itens para maximização dos resultados:

1) Manter pontos de apoio para os drones geograficamente espalhados: para que eles sejam rápidos ao chegar nos locais, é preciso que estejam próximos ao local de destino, com suas baterias carregadas. Este fato de proximidade também maximizaria o tempo de missão, pois sendo o retorno mais próximo é possível que eles se mantenham no ar por mais tempo antes de precisarem recarregar;

2) Configuração correta da distância do ponto de interesse: é preciso que exista um estudo de qual é a distância correta para a primeira aproximação para o caso de cada um dos tipos de eventos, por exemplo, no caso de uma explosão não é aconselhável que o drone se aproxime tanto do local antes de um especialista autorizar, já no caso de uma colisão de automóveis este risco não é tão iminente e é importante a aproximação para identificar se existem ou não vítimas presas nas ferragens;

3) Coordenação aérea com outras aeronaves: existem locais onde o sobrevoo deva ser feito muito cuidadosamente ou até casos onde não seja permitido, por exemplo, na rota de pouso e decolagens em aeroportos, esta situação deve ser considerada corretamente. Outra situação é onde exista um evento de grande repercussão midiática, muitos veículos de cobertura jornalística enviam helicópteros para a região, é preciso ter muita cautela para evitar acidentes entre estas aeronaves;

4) Condições climáticas adversas: é preciso conhecer as corretas características do drone em questão para que ele possa ser utilizado dentro de suas características projetadas. Alguns deles não podem voar com chuva ou ventos de velocidades acima de um determinado limiar;

5) Objetos estacionários perigosos: existem alguns tipos de objetos que podem gerar colisões indesejadas aos drones, tais quais fachadas de prédios e lojas, placas de sinalização e principalmente fios elétricos, cujos estes últimos são muito difíceis de serem identificados por visão computacional;

6) Objetos móveis: é preciso um sistema de detecção de colisões com objetos móveis, principalmente pássaros. Além destes animais, existem possibilidades de colisões em pipas (e suas linhas), balões e até outros drones particulares.

Como benefícios para a utilização de drones pelas forças de segurança, pode-se destacar os seguintes pontos relevantes:

– Tempo de resposta: por estarem próximos, decolarem quase que imediatamente e voarem em linha reta, existe uma grande probabilidade de chegarem muito rapidamente ao ponto de interesse;

– Podem atuar em situações em missões de reconhecimento: como em casos de explosão e incêndio para saber se ainda existe risco iminente de novas explosões ou mesmo desmoronamento;

– Podem prover serviços de apoio: como iluminação noturna ou conectividade de rede em localizações remotas, como buscas de desaparecidos em áreas de florestas ou rurais.

8 CONCLUSÃO

Os métodos de monitoramento de segurança baseados em reconhecimento facial têm a capacidade de realizar um excelente nível de serviço para a sociedade, colaborando para que as cidades inteligentes possam superar os desafios que se apresentam diariamente, desde que sejam projetados e executados de forma eficiente e dentro de parâmetros legais e sociais adequados.

Uma vez que a segurança é uma das necessidades humanas mais importantes, o uso correto de reconhecimento facial permite ampliar a capacidade de monitoramento dos espaços públicos, deixando as ações de proteção mais eficientes.

Com a escolha dos algoritmos mais adequados, como os citados Viola-Jones, Eigenfaces e Fisherfaces, e com o uso correto dentro dos seus parâmetros, é possível desenvolver um sistema eficiente para acompanhamento em tempo real de câmeras e em larga escala.

Com o uso de técnicas de prevenção e os avanços tecnológicos atuais é possível antecipar situações de risco e atuar de forma preventiva sobre elas.

No entanto, quando estes sistemas estiverem funcionando sempre haverá algumas discussões éticas como desafio, como, por exemplo, se o Estado tem o direito de prender uma pessoa futuramente, uma vez que o sistema calculou que as chances dela cometer um crime em breve são grandes, em razão de uma combinação de eventos captados pelo sistema como indicadores de um padrão previamente treinado.

É fundamental entender que é preciso estar apoiado fortemente em iniciativas de controle e liderança para aprimoramento destas aplicações durante sua vida útil, tanto quanto são necessárias a qualidade técnica e o conjunto de boas práticas de arquitetura e desenvolvimento de software. Assim, é possível fazer um serviço de maneira adequada, dentro dos limites éticos e legais da sociedade moderna e democracia atual.

O sistema deve ser projetado para permitir consulta de dados de diversas fontes, utilizando APIs abertas, sendo assim ainda mais eficiente e transparente, possibilitando que outras pessoas possam expandir ainda mais sua capacidade ao agregar módulos complementaremos a ele.

A conexão de diversas fontes de entrada e consulta de dados seria assim possível, como o celular dos policiais que registram imagens desde a abordagem de um suspeito ou um sistema de cadastro de pacientes nos hospitais e abrigos para levantamento de pessoas desaparecidas.

O uso de drones possibilita que se possa sobrevoar grandes quantidades de pessoas e reconhecer diversas imagens em massa em eventos populares.

O sistema necessita permitir informar diferentes movimentos de geração de alertas customizados, com os responsáveis pela pessoa que deve ser encontrada, assim, quando este fato ocorrer é possível saber para onde encaminhá-la e quem deverá ser notificado neste caso.

O sistema deve ter eficiência na armazenagem das imagens capturadas de pessoas em diversos lugares, registrando o histórico de um passado recente para, por exemplo, possibilitar a avaliação de hipóteses policiais, como onde o suspeito esteve em determinado momento e horário.

Armazenar eficientemente as imagens serve para aprimoramento dos recursos públicos e ainda assim garantir o uso das imagens rapidamente no momento que forem requisitadas.

Uma sociedade moderna se constrói com a harmonia entre a tecnologia e os direitos individuais à privacidade. As leis precisam ser reguladas para a utilização destes sistemas, evitando que eles possam ser utilizados para aquisição de dados pessoais como hábitos de consumo, estado de saúde, relacionamentos ou mesmo características pessoais íntimas.

REFERÊNCIAS

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA (ANEEL). **Aneel analisa prazos para as prefeituras se adaptarem às normas sobre iluminação**. Boletim informativo PF/ANEEL. 11. ed. 2015. Disponível em: http://www2.aneel.gov.br/arquivos/HTML/fique_dentro_bip_jan_2015.html. Acesso em: 4 jul. 2016.

AKBAR, M.; RIDHA, M. A. F. SQL injection and cross site scripting prevention using OWASP ModSecurity web application firewall. **JOIV: International Journal on Informatics Visualization**, v. 2, n. 4, p. 286-292, 2018.

ALBAKRI, A. M.; ALMAMORY, S. O.; ALFARTOSY, H. H. Feature-based face detection: a survey. **Iraqi Journal for Computers and Informatics ijci**, v. 44, n. 1, p. 20-26, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **Iluminação pública**: procedimento. ABNT NBR 5101. Rio de Janeiro: ABNT, 1992.

AVER, A. A relação Iluminação Pública e Criminalidade. **Revista Especialize**, 2013. Disponível em: http://www.bussinesstour.com.br/uploads/arquivos/7e766f5534244d2d51fc7fe1b55f9444.pdf. Acesso em: 6 jun. 2016.

BBC CLICK. **Are you ready for a world of facial recognition?** Several UK police forces have been trialling the technology. Twitter, 13 maio 2019. Disponível em: https://twitter.com/BBCClick/status/1127961872286789634

BELHUMEUR, P. N.; HESPANHA, J. P.; KRIEGMAN, D. J. Eigenfaces vs. fisherfaces: recognition using class specific linear projection. **IEEE Transactions on Pattern Analysis & Machine Intelligence**, n. 7, p. 711-720, 1997.

BETARTE, G.; PARDO, Á.; MARTÍNEZ, R. Web application attacks detection using machine learning techniques. **17th IEEE International Conference on Machine Learning and Applications (ICMLA)**, p. 1.065-1.072, 2018.

BISSI, T. **Reconhecimento facial com os algoritmos eigenfaces e fisherfaces**. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Universidade Federal de Uberlândia, Uberlândia, MG, 2018.

CALAVIA, L. et al. A semantic autonomous video surveillance system for dense camera networks in smart cities. **Sensors**, v. 12, n. 8, p. 10.407-10.429, 2012.

CARVALHO, A. H. P. Segurança de aplicações web e os dez anos do relatório OWASP Top Ten: o que mudou? **Fasci-Tech**, v. 1, n. 8, p. 6-18, 2014.

CASTRO, F. N.; LUCIANO, B. A. Eficiência energética em sistemas de iluminação pública. **O setor elétrico**. v. 7., p. 38-47, 2012.

CHOURABI, H. et al. Understanding smart cities: an integrative framework. In: SYSTEM SCIENCE (HICSS), 2012, **45th Hawaii International Conference on IEEE**, p. 2.289-2.297, 2012.

CLARKE, R. V.; ECK, J. E. **Análise de crime para solucionadores de problemas em 60 pequenos passos**. Publisher: Departamento de Justiça dos EUA, 2005. Disponível em: https://popcenter.asu.edu/sites/default/files/library/reading/PDFs/60steps-portuguese.pdf. Acesso em: 14 jun. 2016.

CERT.br. **Home**. Disponível em: https://www.cert.br/. Acesso em: 24 fev. 2019.

DANTAS, G. F. L. **Algumas considerações básicas acerca da moderna "Análise Criminal"**. Disponível em: https://www.scribd.com/document/147881649/ALGUMAS-CONSIDERACOES-BASICAS-ACERCA-DA-MODERNA-ANALISE-CRIMINAL#download. Acesso em: 2 jul. 2019.

DASTIN, Jeffrey. **Amazon scraps secret AI recruiting tool that showed bias against women**. Reuters, 10 out. 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

FARRINGTON, D. P.; WELSH, B. C. Effects of improved street lighting on crime: a systematic review, 2003. **Home Office Research Study 251**. Disponível em: https://keysso.net/community_news/May_2003/improved_lighting_study.pdf. Acesso em: 17 abr. 2014.

FERRAZ, F. et al. Towards a smart city security model exploring smart cities elements based on nowadays solutions. In: ICSEA 2013. **The Eighth International Conference on Software Engineering Advances**. p. 546-550, 2013.

FREUND, Y.; SCHAPIRE, R. E. Experiments with a new boosting algorithm. **ICML**, v. 96, p. 148-156, 1996.

GOLDSTEIN, H. Improving policing: a problem oriented approach. **Crime and delinquency 25**, p. 244-245, 1979.

GREENGARD, S. Policing the future. **Communications of the ACM**, v. 55, n. 3, p. 19-21, 2012.

HABITAT III. ONU Habitat. **Cidades inteligentes**. Disponível em: https://www.habitat3.org/bitcache/7cab8d607dffc68f07513d59fdcfa29a241babe1?vid=581165&disposition=inline&op=view. Acesso em: 3 jun. 2016.

HART, T. C.; ZANDBERGEN, P. A. Effects of data quality on predictive hotspot mapping. **Research Gate**, jan. 2012.

HEFENBROCK, D.; OBERG, J.; THANH, N. T. N.; KASTNER, R.; BADEN, S. B. Accelerating Viola-Jones face detection to fpga-level using gpus. **18th IEEE annual international symposium on field-programmable custom computing machines**, p. 11-18, 2010.

HEGDE, N.; PREETHA, S.; BHAGWAT, S. Facial expression classifier using better technique: fisherface algorithm. **2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI)**, p. 604-610, 2018.

IBM. **Smarter cities**. Disponível em: http://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/. Acesso em: 3 maio 2014.

INDEX MUNDI. **World demographics profile**. 2012.

JIA, Kai; KENNEY, Martin; MATTILA, Juri; SEPPÄLÄ, Timo. **The application of artificial intelligence at chinese digital platform giants**: Baidu, Alibaba and Tencent. ETLA Reports, n. 81, 26 fev. 2018. Disponível em: https://pub.etla.fi/ETLA-Raportit-Reports-81.pdf.

JUNG, M. et al. Building automation and smart cities: an integration approach based on a service-oriented architecture. In: Advanced Information Networking and Applications Workshops (WAINA). **27th International Conference on IEEE**, p. 1361-1367, 2013.

LI, Ya et al. Distance metric optimization driven convolutional neural network for age invariant face recognition. **Pattern Recognition**, v. 75, p. 51-62, 2018.

LIU, Joyce. **In your face**: China's all-seeing state. BBC News, 10 dez. 2017. Disponível em: https://www.bbc.com/news/av/world-asia-china-42248056/in-your-face-china-s-all-seeing-state

LOHR, Steve. **Facial recognition is accurate, if you're a white guy**. The New York Times, 9 fev. 2018. Disponível em: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html

MACHADO, F. **Brasil perde US$ 10 bilhões por ano com cibercrime, diz McAfee**. Revista Veja, 21 fev. 2018. Disponível em: https://veja.abril.com.br/economia/brasil-perde-us-10-bilhoes-por-ano-com-cibercrime-diz-mcafee/. Acesso em: 21 fev. 2018.

MARCHANT, P. What is the contribution of street lighting to keeping us safe? An investigation into a policy. **Radical Statistics**, Issue 102, 2010. Disponível em: http://www.radstats.org.uk/no102/Marchant102.pdf. Acesso em: 23 abr. 2014.

MARR, B. **20 fatos sobre a internet que você (provavelmente) não sabe**. Forbes, 2015. Disponível em: http://www.forbes.com.br/fotos/2015/10/20-fatos-

sobre-a-internet-que-voce-provavelmente-nao-sabe/#foto2. Acesso em: 8 jun. 2016.

MARTINI, S. **Sistema integrado de gestão da infraestrutura urbana**. 2013. Disponível em: http://ie.org.br/site/ieadm/arquivos/arqnot8136.pdf. Acesso em: 19 maio 2016.

MARTINS, J. O papel social da luz urbana. **O setor elétrico**. 69 ed., 2011. Disponível em: http://www.osetoreletrico.com.br/web/component/content/article/57-artigos-e-materias/745-o-papel-social-da-luz-urbana.html. Acesso em: 8 jun. 2016.

MASCARO, L. **A iluminação do espaço urbano**. Porto Alegre: Masquatro, 2006.

MASLOW, A. H. A theory of human motivation. **Psychological Review**, n. 50, p. 390-396, 1943.

MIT. **Cidade da ciência**. Disponível em: http://cities.media.mit.edu/. Acesso em: 3 maio 2014.

MONTEVERDE, W.; CAMPIOLO, R. Estudo e análise de vulnerabilidades web. **XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais – SBSeg 2014**, Belo Horizonte, 3 a 6 nov. 2014.

MUHAMMAD, Khan; AHMAD, Jamil; BAIK, Sung Wook. Early fire detection using convolutional neural networks during surveillance for effective disaster management. **Neurocomputing**, v. 288, p. 30-42, 2018.

OLIVEIRA, T. S. T. **Testes de segurança em aplicações web segundo a metodologia OWASP**. 126 p. Monografia (Graduação em Ciência da Computação) – Universidade Federal de Lavras, Lavras, MG, 2012.

PAN, G. et al. Trace analysis and mining for smart cities: issues, methods, and applications. **IEEE Communications Magazine**, p. 121, 2013.

PECLAT, R. N.; RAMOS, G. N. Identificação automatizada de riscos de segurança em especificações de software. **Workshop da Pós-Graduação em Computação – WPOS 2014**, Pirenópolis, GO, 2014.

PERERA, C. et al. Sensing as a service model for smart cities supported by internet of things. **Transactions on Emerging Telecommunications Technologies**, 2013.

PHILIPS. **Luminárias inteligente para iluminação rodoviária com ligação plug & play**. Disponível em: http://www.lighting.philips.pt/prof/luminarias-de-exterior/road-and-urban-lighting/road-and-urban-luminaires/iridium-gen3-led/iridium-gen3-led-large. Acesso em: 19 maio 2016.

ROCHE, S. et al. Are “smart cities” smart enough. In: **Global Geospatial Conference**, 2012.

ROIZENBLATT, I. **Critérios da iluminação elétrica urbana**. Tese (Doutorado em Arquitetura e Urbanismo) – Universidade Presbiteriana Mackenzie, São Paulo, 2009.

ROSITO, L. H. **As origens da iluminação pública no Brasil**. 2009. Disponível em: http://www.osetoreletrico.com.br. Acesso em: 6 jun. 2016.

SAGAR, D.; KUKREJA, S.; BRAHMA, J.; TYAGI, S.; JAIN, P. Studying open source vulnerability scanners for vulnerabilities in web applications. **IIOAB JOURNAL**, v. 9, n. 2, p. 43-49, 2018.

SAJJAD, Muhammad et al. Raspberry Pi assisted facial expression recognition framework for smart security in law-enforcement services. **Information Sciences**, v. 479, p. 416-431, 2019.

SANTOS, E.; NUNES, R. Avaliando a importância das metodologias para aplicação de testes de segurança em sistemas de informação. **Workshop de Trabalhos de Iniciação Científica e de Graduação – WTICG**, Instituto Federal de Santa Catarina, 2014.

SECRETARIA DA SEGURANÇA PÚBLICA. **Sistema de inteligência criam o mapa da criminalidade**. Disponível em: http://www.ssp.sp.gov.br/acoes/acoes_sistemas.aspx. Acesso em: 10 jun. 2016.

SHEKHAR, S. et al. Crime pattern analysis: a spatial frequent pattern mining approach. **Minnesota University Minneapolis Dept Of Computer Science And Engineering**, 2012.

SINGER, Natasha. **Amazon’s facial recognition wrongly identifies 28 lawmakers, A.C.L.U. says**. The New York Times, 26 jul. 2018. Disponível em: https://www.nytimes.com/2018/07/26/technology/amazon-aclu-facial-recognition-congress.html

SOUZA, L. L. **Desenvolvimento seguro de aplicações web segundo a metodologia OWASP**. Monografia (Graduação em Ciência da Computação) – Universidade Federal de Lavras, Lavras, MG, 2012.
SAS. **Big Data**: o que é e qual sua importância? Disponível em: http://www.sas.com/pt_br/insights/big-data/what-is-big-data.html. Acesso em: 7 jun. 2016.

STACK OVERFLOW. **Multi resolution discrete wavelet 3d plot in matlab**. Disponível em: http://stackoverflow.com/questions/12684277/multiresolution-discrete-wavelet-3d-plot-in-matlab. Acesso em: 3 maio 2014.

TASTE OF SUSTAINABILITY. **Rent Heat Map**. Disponível em: http://www.tasteofsustainability.com/rent_heat_map/apts_20130323.png. Acesso em: 3 maio 2014.

TAURION, C. Software embarcado: a nova onda da informática. **Brasport**, 2005.

THE ECONOMIST. **China**: facial recogniton and state control. YouTube, 24 out. 2018. Disponível em: https://www.youtube.com/watch?v=lH2gMNrUuEY

THE SOCIAL PROGRESS IMPERATIVE. **Índice de progresso social**. Disponível em: http://www.socialprogressimperative.org/pt/data/spi/countries/BRA#data_table/components/BRA/. Acesso em: 3 abr. 2014.

TREGENZA, P.; LOE, D. **Projeto de iluminação**. 2. ed. Porto Alegre: Bookman, 2015.

TURK, M. A.; PENTLAND, A. P. Face recognition using eigenfaces. In: **Proceedings 1991 IEEE Computer Society Conference on Computer Vision and Pattern Recognition**, p. 586-591, 1991.

UOL. **Brasil tem 16 cidades entre as 50 mais violentas do mundo, diz ong mexicana**. Disponível em: http://noticias.uol.com.br/internacional/ultimas-noticias/2014/01/17/brasil-tem-16-cidades-entre-as-50-mais-violentas-do-mundo-diz-ong-mexicana.htm. Acesso em: 3 maio 2014.

USP. **Mapa da cidade universitária**. Disponível em: http://www.usp.br/mapas/mapas/pdf/cidadeuniversitaria.pdf. Acesso em: 3 maio 2014.

VIOLA, P.; JONES, M. Rapid object detection using a boosted cascade of simple features. **Null**, n. 511, 2001.

WIKI COMMONS. **Imagem noturna da estufa principal do Jardim Botânico de Curitiba, PR, Sul do Brasil**. Samir Nosteb, 2009. Disponível em: https://commons.wikimedia.org/wiki/File:JardimBotanicoCuritibaNoite.1.JPG. Acesso em: 7 jun. 2016.

WILSON, M. **By 2050, 70% of the world's population will be urban. Is that a good thing?** Fast Company, 2012. Disponível em: https://www.fastcompany.com/1669244/by-2050-70-of-the-worlds-population-will-be-urban-is-that-a-good-thing. Acesso em:

WRIGHT, John et al. Robust face recognition via sparse representation. **IEEE transactions on pattern analysis and machine intelligence**, v. 31, n. 2, p. 210-227, 2008.

YU, Chunyu; MEI, Zhibin; ZHANG, Xi. A real-time video fire flame and smoke detection algorithm. **Procedia Engineering**, v. 62, p. 891-898, 2013.

APÊNDICE A – Codificação das regras de referência com a lógica Fuzzy

Abaixo a exemplificação do código-fonte de detalhamento do mapa de risco em Lógica Fuzzy

if Iluminacao is Boa and Transito is Intenso and Historico is BaixaIncidencia then Periculosidade is Baixa
if Iluminacao is Boa and Transito is Intenso and Historico is MediaIncidencia then Periculosidade is Atencao
if Iluminacao is Boa and Transito is Intenso and Historico is AltaIncidencia then Periculosidade is Atencao
if Iluminacao is Boa and Transito is Normal and Historico is BaixaIncidencia then Periculosidade is Baixa
if Iluminacao is Boa and Transito is Normal and Historico is MediaIncidencia then Periculosidade is Baixa
if Iluminacao is Boa and Transito is Normal and Historico is AltaIncidencia then Periculosidade is Baixa
if Iluminacao is Boa and Transito is Vazio and Historico is BaixaIncidencia then Periculosidade is Baixa
if Iluminacao is Boa and Transito is Vazio and Historico is MediaIncidencia then Periculosidade is Baixa
if Iluminacao is Boa and Transito is Vazio and Historico is AltaIncidencia then Periculosidade is Atencao
if Iluminacao is Regular and Transito is Intenso and Historico is BaixaIncidencia then Periculosidade is Baixa
if Iluminacao is Regular and Transito is Intenso and Historico is MediaIncidencia then Periculosidade is Atencao
if Iluminacao is Regular and Transito is Intenso and Historico is AltaIncidencia then Periculosidade is Alta
if Iluminacao is Regular and Transito is Normal and Historico is BaixaIncidencia then Periculosidade is Baixa
if Iluminacao is Regular and Transito is Normal and Historico is MediaIncidencia then Periculosidade is Baixa
if Iluminacao is Regular and Transito is Normal and Historico is AltaIncidencia then Periculosidade is Baixa
if Iluminacao is Regular and Transito is Vazio and Historico is BaixaIncidencia then Periculosidade is Baixa
if Iluminacao is Regular and Transito is Vazio and Historico is MediaIncidencia then Periculosidade is Baixa
if Iluminacao is Regular and Transito is Vazio and Historico is AltaIncidencia then Periculosidade is Atencao
if Iluminacao is Ruim and Transito is Intenso and Historico is BaixaIncidencia then Periculosidade is Atencao
if Iluminacao is Ruim and Transito is Intenso and Historico is MediaIncidencia then Periculosidade is Alta
if Iluminacao is Ruim and Transito is Intenso and Historico is AltaIncidencia then Periculosidade is Alta
if Iluminacao is Ruim and Transito is Normal and Historico is BaixaIncidencia then

Periculosidade is Baixa
if Iluminacao is Ruim and Transito is Normal and Historico is MediaIncidencia then Periculosidade is Atencao
if Iluminacao is Ruim and Transito is Normal and Historico is AltaIncidencia then Periculosidade is Atencao
if Iluminacao is Ruim and Transito is Vazio and Historico is BaixaIncidencia then Periculosidade is Atencao
if Iluminacao is Ruim and Transito is Vazio and Historico is MediaIncidencia then Periculosidade is Atencao
if Iluminacao is Ruim and Transito is Vazio and Historico is AltaIncidencia then Periculosidade is Alta

APÊNDICE B – Modelo matemático de periculosidade em lógica Fuzzy

Algoritmo que implementa o modelo matemático em Lógica Fuzzy escrito em Java com a biblioteca fuzzylite, onde se definem os valores de entrada e saídas das variáveis bem como as regras de inferência devem funcionar na presença de determinadas variáveis de entrada implicar qual valor na variável de saída.

```
import com.fuzzylite.Engine;
import com.fuzzylite.FuzzyLite;
import com.fuzzylite.defuzzifier.Centroid;
import com.fuzzylite.imex.FldExporter;
import com.fuzzylite.norm.s.Maximum;
import com.fuzzylite.norm.t.Minimum;
import com.fuzzylite.rule.Rule;
import com.fuzzylite.rule.RuleBlock;
import com.fuzzylite.term.Triangle;
import com.fuzzylite.variable.InputVariable;
import com.fuzzylite.variable.OutputVariable;

public class Periculosidade {


   public static void main(String[] args){


        Engine = new Engine();
        engine.setName("Periculosidade");
        engine.configure("", "", "Minimum", "Maximum", "Centroid");


        InputVariable inputVariable1 = new InputVariable();
        inputVariable1.setEnabled(true);
        inputVariable1.setName("Iluminacao");
        inputVariable1.setRange(0.000, 1.000);
        inputVariable1.addTerm(new Triangle("Boa", 0.600, 1.000, 1.000));
        inputVariable1.addTerm(new Triangle("Regular", 0.250, 0.500, 0.750));
        inputVariable1.addTerm(new Triangle("Ruim", 0.000, 0.000, 0.400));
        engine.addInputVariable(inputVariable1);


        InputVariable inputVariable2 = new InputVariable();
        inputVariable2.setEnabled(true);
        inputVariable2.setName("Transito");
        inputVariable2.setRange(0.000, 1.000);
        inputVariable2.addTerm(new Triangle("Intenso", 0.600, 1.000, 1.000));
```

```
        inputVariable2.addTerm(new Triangle("Normal", 0.250, 0.500, 0.750));
        inputVariable2.addTerm(new Triangle("Vazio", 0.000, 0.000, 0.400));
        engine.addInputVariable(inputVariable2);
        InputVariable inputVariable3 = new InputVariable();
        inputVariable3.setEnabled(true);
        inputVariable3.setName("Historico");
        inputVariable3.setRange(0.000, 1.000);
        inputVariable3.addTerm(new Triangle("AltaIncidencia", 0.600, 1.000,
1.000));
        inputVariable3.addTerm(new Triangle("MediaIncidencia", 0.250, 0.500,
0.750));
        inputVariable3.addTerm(new Triangle("BaixaIncidencia", 0.000, 0.000,
0.400));
        engine.addInputVariable(inputVariable3);


        OutputVariable = new OutputVariable();
        outputVariable.setEnabled(true);
        outputVariable.setName("Periculosidade");
        outputVariable.setRange(0.000, 1.000);
        outputVariable.fuzzyOutput().setAccumulation(new Maximum());
        outputVariable.setDefuzzifier(new Centroid(200));
        outputVariable.setDefaultValue(Double.NaN);
        outputVariable.addTerm(new Triangle("Alta", 0.500, 0.750, 1.000));
        outputVariable.addTerm(new Triangle("Atencao", 0.250, 0.500, 0.750));
        outputVariable.addTerm(new Triangle("Baixa", 0.000, 0.250, 0.500));
        engine.addOutputVariable(outputVariable);

        RuleBlock = new RuleBlock();
        ruleBlock.setEnabled(true);
        ruleBlock.setName("");
        ruleBlock.setConjunction(new Minimum());
        ruleBlock.setDisjunction(new Maximum());
        ruleBlock.setActivation(new Minimum());

        ruleBlock.addRule(Rule.parse("if Iluminacao is Boa and Transito is Intenso
and Historico is BaixaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Boa and Transito is Intenso
and Historico is MediaIncidencia then Periculosidade is Atencao", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Boa and Transito is Intenso
and Historico is AltaIncidencia then Periculosidade is Atencao", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Boa and Transito is Normal
and Historico is BaixaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Boa and Transito is Normal
and Historico is MediaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Boa and Transito is Normal
and Historico is AltaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Boa and Transito is Vazio
and Historico is BaixaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Boa and Transito is Vazio
```

```
and Historico is MediaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Boa and Transito is Vazio
and Historico is AltaIncidencia then Periculosidade is Atencao", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Regular and Transito is
Intenso and Historico is BaixaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Regular and Transito is
Intenso and Historico is MediaIncidencia then Periculosidade is Atencao",
engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Regular and Transito is
Intenso and Historico is AltaIncidencia then Periculosidade is Alta", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Regular and Transito is
Normal and Historico is BaixaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Regular and Transito is
Normal and Historico is MediaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Regular and Transito is
Normal and Historico is AltaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Regular and Transito is
Vazio and Historico is BaixaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Regular and Transito is
Vazio and Historico is MediaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Regular and Transito is
Vazio and Historico is AltaIncidencia then Periculosidade is Atencao", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Ruim and Transito is
Intenso and Historico is BaixaIncidencia then Periculosidade is Atencao",
engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Ruim and Transito is
Intenso and Historico is MediaIncidencia then Periculosidade is Alta", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Ruim and Transito is
Intenso and Historico is AltaIncidencia then Periculosidade is Alta", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Ruim and Transito is
Normal and Historico is BaixaIncidencia then Periculosidade is Baixa", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Ruim and Transito is
Normal and Historico is MediaIncidencia then Periculosidade is Atencao",
engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Ruim and Transito is
Normal and Historico is AltaIncidencia then Periculosidade is Atencao", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Ruim and Transito is Vazio
and Historico is BaixaIncidencia then Periculosidade is Atencao", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Ruim and Transito is Vazio
and Historico is MediaIncidencia then Periculosidade is Atencao", engine));
        ruleBlock.addRule(Rule.parse("if Iluminacao is Ruim and Transito is Vazio
and Historico is AltaIncidencia then Periculosidade is Alta", engine));
        engine.addRuleBlock(ruleBlock);
        inputVariable1.setInputValue(0.1);
        inputVariable2.setInputValue(0.1);
        inputVariable3.setInputValue(0.1);
        FuzzyLite.logger().info(new FldExporter().toString(engine));

    }
}
```