UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA
INSTITUTO TÉRCIO PACITTI DE APLICAÇÕES E PESQUISAS COMPUTACIONAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

ROSEMBERGUE PEREIRA DE SOUZA

UM ARCABOUÇO TECNOLÓGICO PARA DETECÇÃO DE POSSÍVEIS SERVIÇOS FRAUDULENTOS EM ORGANISMOS DE AVALIAÇÃO DA CONFORMIDADE

Rio de Janeiro
2017

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA
INSTITUTO TÉRCIO PACITTI DE APLICAÇÕES E PESQUISAS COMPUTACIONAIS
PROGRAMA DE PÓS-GRADUAÇÃO EM INFORMÁTICA

ROSEMBERGUE PEREIRA DE SOUZA

UM ARCABOUÇO TECNOLÓGICO PARA DETECÇÃO DE POSSÍVEIS SERVIÇOS FRAUDULENTOS EM ORGANISMOS DE AVALIAÇÃO DA CONFORMIDADE

Tese de Doutorado submetida ao Corpo Docente do Departamento de Ciência da Computação do Instituto de Matemática, e Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para obtenção do título de Doutor em Informática.

Orientador: Luiz Fernando Rust da Costa Carmo, UFRJ
Co-orientador: Luci Pirmez, UFRJ

Rio de Janeiro
2017

CBIB Souza, Rosembergue Pereira de

Um arcabouço tecnológico para detecção de possíveis serviços fraudulentos em organismos de avaliação da conformidade / Rosembergue Pereira de Souza. – 2017.
168 f.: il.

Tese de Doutorado em Informática – Universidade Federal do Rio de Janeiro, Instituto de Matemática, Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Programa de Pós-Graduação em Informática, Rio de Janeiro, 2017.

Orientador: Luiz Fernando Rust da Costa Carmo, UFRJ.
Co-orientador: Luci Pirmez, UFRJ.

1. Avaliação da conformidade. 2. Detecção de fraudes. 3. Aprendizado de máquina. 4. Visão computacional. – Tese de Doutorado. I. Carmo, UFRJ, Luiz Fernando Rust da Costa (Orient.). II. Pirmez, UFRJ, Luci (Co-orient.). III. Universidade Federal do Rio de Janeiro, Instituto de Matemática, Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Programa de Pós-Graduação em Informática.

CDD

ROSEMBERGUE PEREIRA DE SOUZA

Um arcabouço tecnológico para detecção de possíveis serviços fraudulentos em organismos de avaliação da conformidade

Tese de Doutorado submetida ao Corpo Docente do Departamento de Ciência da Computação do Instituto de Matemática, e Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais da Universidade Federal do Rio de Janeiro, como parte dos requisitos necessários para obtenção do título de Doutor em Informática.

Aprovado em: Rio de Janeiro, 13 de dezembro de 2017.

Prof. Dr. Luiz Fernando Rust da Costa Carmo, UFRJ (Orientador)

Profª. Drª. Luci Pirmez, UFRJ (Co-orientadora)

Profª. Drª. Priscila Machado Vieira Lima, UFRJ

Prof. Dr. Raphael Carlos Santos Machado, Inmetro

Prof. Dr. Altair Olivo Santin, PUCPR

Aos meus pais, familiares e amigos.

AGRADECIMENTOS

Agradeço a Deus, aos meus pais e familiares, ao meu orientador e minha co-orientadora, aos meus amigos e ao Inmetro por todo apoio.

RESUMO

Souza, Rosembergue Pereira de. **Um arcabouço tecnológico para detecção de possíveis serviços fraudulentos em organismos de avaliação da conformidade**. 2017. 152 f. Tese de Doutorado em Informática - PPGI, Instituto de Matemática, Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017.

Avaliação da Conformidade é a demonstração de que os requisitos especificados relativos a um produto, processo, sistema, pessoa ou organismo são atendidos. Este método faz com que os produtos e serviços atendam aos objetivos que se pretendem. Ferramentas de avaliação da conformidade são ensaio, certificação, inspeção e acreditação. Fraudes em serviços de avaliação da conformidade trazem sérios riscos à segurança e à saúde da população, bem como ao meio ambiente. Além disso, a realização de serviços de avaliação da conformidade de forma fraudulenta representa um tratamento desleal e ilegal por parte daqueles que se valem de produtos adulterados para ganhos sobre o consumidor. Neste trabalho, propõe-se um arcabouço para identificar possíveis casos de fraude nos serviços prestados por organismos de avaliação da conformidade. Este arcabouço compreende uma técnica de monitoramento de vários centros de avaliação da conformidade e técnicas para detectar possíveis fraudes em um organismo de avaliação da conformidade. Também, incorporam esse arcabouço técnicas para análise rápida de vídeos desses organismos de avaliação da conformidade para monitorar fraudes e uma técnica baseada em assinaturas para investigação automática de fraudes em organismos de avaliação da conformidade. Nos experimentos, focou-se na ferramenta de inspeção e o arcabouço proposto conseguiu identificar com sucesso as organizações com comportamento fraudulento.

Palavras-chave: Avaliação da conformidade, Detecção de fraudes, Aprendizado de máquina, Visão computacional.

ABSTRACT

Souza, Rosembergue Pereira de. **Um arcabouço tecnológico para detecção de possíveis serviços fraudulentos em organismos de avaliação da conformidade**. 2017. 152 f. Tese de Doutorado em Informática - PPGI, Instituto de Matemática, Instituto Tércio Pacitti de Aplicações e Pesquisas Computacionais, Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2017.

Conformity assessment is a method for demonstrating that an object's features meet the criteria of standards, regulations and other specifications. This method ensures that products and services deliver on their promises. The toolbox of conformity assessment includes testing, inspection, certification and accreditation. Fraudulent behavior in conformity assessment process generates dangerous products to the ordinary citizen and environment. Also, this kind of behavior produces unfair competition between conformity assessment bodies. In this work, we presented a framework to detect possible fraudulent behavior in conformity assessment bodies. This framework comprehends a method for monitoring multicenter conformity assessment bodies and techniques to detect suspected fraud by an conformity assessment body. Also, there are techniques to rapid video assessment for monitoring conformity assessment body fraud and a signature based method for automatically investigating possible fraudulent behavior in conformity assessment bodies. In the experiments, the focus was the inspection tool and the conformity assessment bodies with fraudulent behavior were successfully detected by the proposed framework.

Keywords: Conformity assessment, Fraud detection, Machine learning, Computer vision.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Avaliação da conformidade

Avaliação da Conformidade é a demonstração de que os requisitos especificados relativos a um produto, processo, sistema, pessoa ou organismo são atendidos (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2004). Existem diversos tipos de ferramentas de avaliação da conformidade, a saber: ensaio, inspeção, certificação e acreditação. As empresas que realizam essas atividades são chamadas de organismos de avaliação da conformidade (OAC).

Para as organizações empresariais, a avaliação da conformidade induz à busca contínua da melhoria da qualidade, tornando a concorrência mais justa, na medida em que indica, claramente, os produtos, processos ou serviços que atendem aos requisitos especificados. Por sua vez, para o Estado Regulador, a adoção da avaliação da conformidade, no âmbito compulsório, é uma ferramenta que fortalece o poder regulatório das instituições públicas, sendo um instrumento eficiente de proteção à saúde e segurança do consumidor e ao meio ambiente (INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA, 2007).

A Figura 1.1 mostra o fluxograma do processo de avaliação da conformidade. A abordagem da avaliação de conformidade denota-se por uma série de três funções: seleção; determinação; e análise crítica e atestação. Uma vez determinada a necessidade de se verificar o atendimento a determinados requisitos, o primeiro passo consiste na seleção do objeto que terá sua conformidade avaliada.

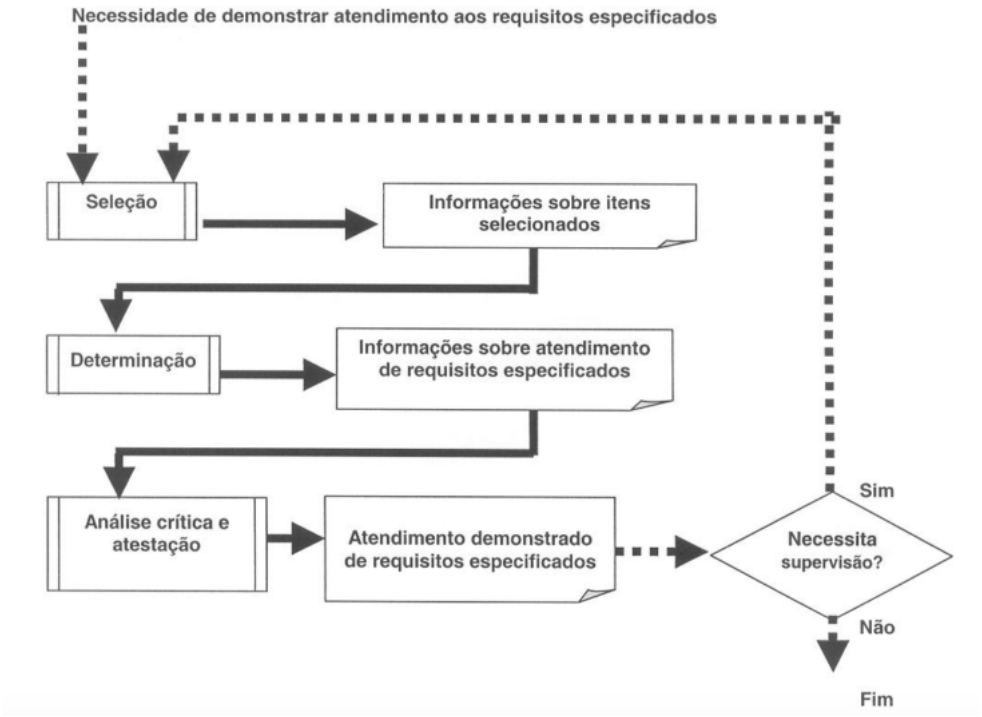


Figura 1.1: Fluxograma do processo de avaliação da conformidade (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2004)

A seleção envolve as atividades de planejamento e preparação, de forma a coletar todas as informações e entradas necessárias para a função determinação subsequente. Frequentemente, o objeto pode ser um grande número de itens idênticos, produção em andamento, um processo contínuo ou um sistema, ou pode envolver diversas localidades. Nesses casos, considerações podem ser feitas sobre a amostragem ou seleção de amostras a serem usadas nas atividades de determinação. Todas as informações, amostras (se for usada amostragem), decisões e outra saída da função seleção são representadas como "informações sobre itens selecionados".

Na etapa de determinação, atividades são conduzidas para desenvolver informações completas relativas ao atendimento aos requisitos especificados pelo objeto

da avaliação de conformidade ou sua amostra. Alguns tipos de atividades de determinação são ensaio , inspeção , certificação e avaliação entre pares. Todas as saídas da função determinação são representadas como "informações sobre atendimento de requisitos especificados". A saída é a combinação de todas as informações geradas através da atividade de determinação, bem como todas as entradas para a função determinação. A saída é normalmente estruturada para facilitar as atividades de análise crítica e atestação.

Em seguida, tem-se etapa de análise crítica e atestação, que é a verificação do atendimento aos requisitos especificados, concatenada com a fase de atestação que consiste em uma afirmação da conformidade do objeto avaliado. Todas as saídas da função análise crítica e atestação são representadas como "atendimento demonstrado de requisitos especificados".

Por fim, verifica-se se há necessidade de supervisão. As atividades exercidas na supervisão são planejadas de forma a satisfazer o requisito de manter a validade de uma afirmação existente resultante de uma atestação (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2004).

1.2 Acreditação

Para que exista confiança nos resultados de um organismo de avaliação da conformidade, usa-se o mecanismo da acreditação. Acreditação é a atestação realizada por terceira parte relativa a um organismo de avaliação da conformidade, exprimindo demonstração formal de sua competência para realizar tarefas específicas de avaliação da conformidade (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2004).

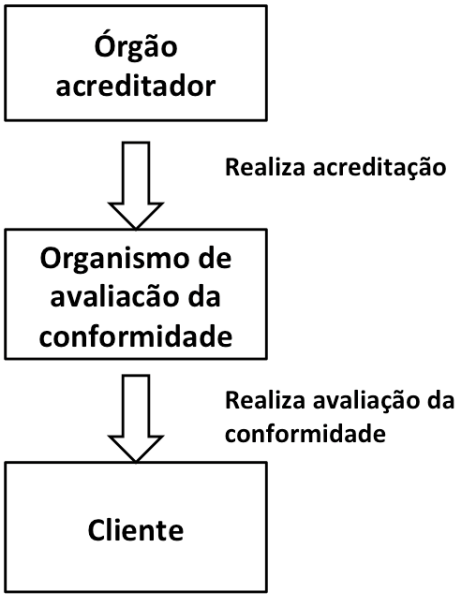


Figura 1.2: Hierarquia do processo de avaliação da conformidade.

No Brasil, o acreditador oficial é a Coordenação Geral de Acreditação do Inmetro (CGCRE). Uma vez que a organização solicitante é acreditada, a CGCRE realiza avaliações de supervisão para verificar se essa empresa continua mantendo as condições técnicas e regulamentares para prestar o serviço acreditado. Nessas supervisões, os avaliadores da CGCRE verificam as condições das instalações e equipamentos do organismo, bem como a competência técnica do pessoal e capacidade de gestão da empresa. Além disso, a equipe da CGCRE verifica os registros dos serviços prestados pela a organização acreditada. Esta análise investiga se o organismo prestou serviços conforme os regulamentos técnicos pertinentes.

A Figura 1.2 mostra hierarquia do processo de avaliação da conformidade. O órgão acreditador realiza a acreditação e supervisiona os organismos de avaliação da conformidade acreditados. Por sua vez, os organismos de avaliação da conformidade avaliam os produtos de seus clientes para verificar se atendem a requisitos especifi-

cados. Quando o órgão acreditador recebe uma reclamação sobre casos de fraude, ele deve realizar uma investigação para verificar o cumprimento de regulamentos técnicos e também apurar a procedência da reclamação.

1.3 Apresentação do problema

As fraudes em serviços de avaliação da conformidade consistem na emissão de relatórios e certificados sem que os serviços de avaliação da conformidade tenham sido realizados; com manipulação de resultados; emissão de certificados ou relatórios por profissional não habilitado; falsificação de registros ou outras informações (INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA, 2017).

A realização de serviços de avaliação da conformidade de forma fraudulenta representa um tratamento desleal e ilegal por parte daqueles que se valem de produtos adulterados para ganhos sobre o consumidor. Como exemplo, pode-se citar o caso das inspeções periódicas realizadas em equipamentos que transportam produtos perigosos no Brasil. A existência de fraude nessas inspeções leva a possível circulação de equipamentos inseguros pelas ruas e estradas transportando material nocivo ao meio ambiente, tais equipamentos podem ser envolvidos em acidentes causando vítimas fatais e poluição da natureza. Desta forma, torna-se necessário, o monitoramento dessas fraudes no mercado, para que se possa agir de modo mais eficaz inibindo a propagação de tais práticas.

A Figura 1.3 mostra uma lista de tipos de fraudes que ocorrem no âmbito da avaliação da conformidade com relação aos organismos acreditados e seus clientes. As fraudes em serviços de avaliação da conformidade podem ser divididas em fraudes do organismo que realiza o serviço e fraudes dos clientes desses organismos. A

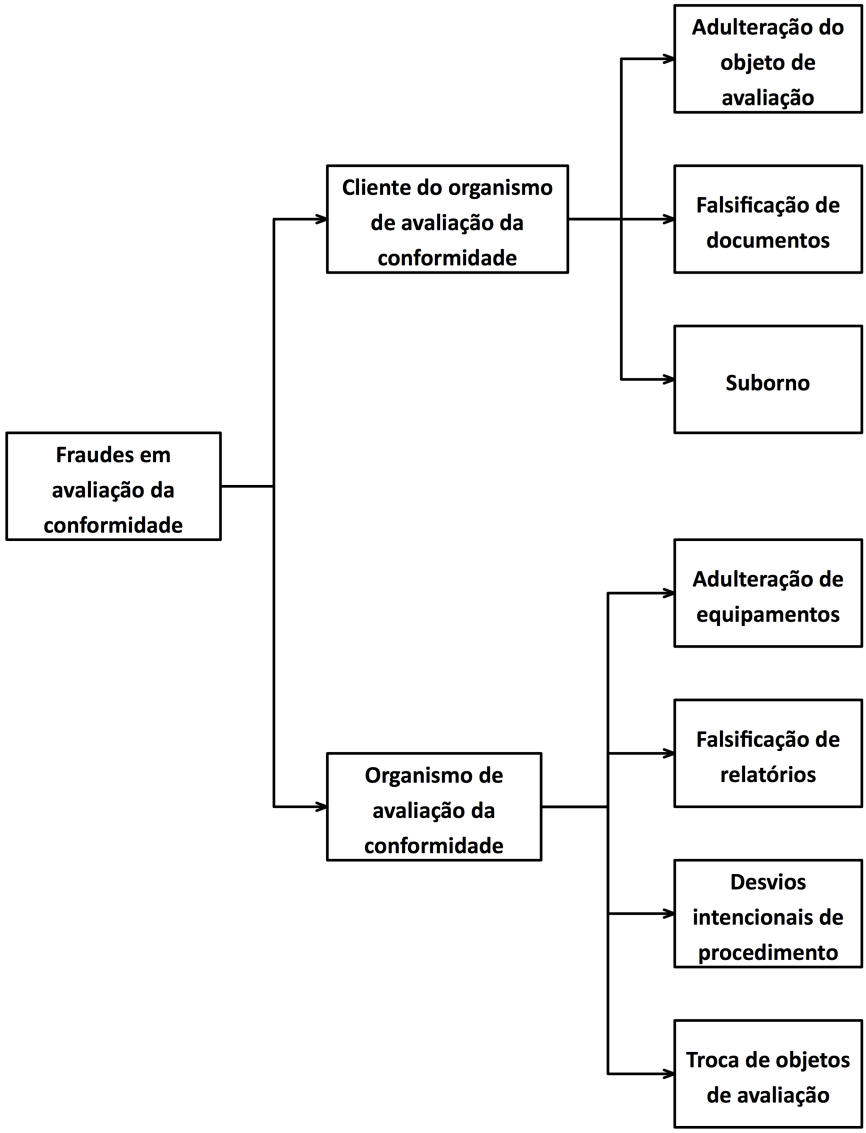


Figura 1.3: Tipos de fraudes que ocorrem no âmbito da avaliação da conformidade com relação aos organismos acreditados e seus clientes.

principal motivação para o organismo de avaliação da conformidade realizar fraudes em seus serviços consiste em uma expectativa de ganhos financeiros. Além de evitar conflitos com seus clientes. Para isso, essas organizações fraudulentas podem: i) adulterar seus equipamentos de modo a apresentarem medições que acordo com a conveniência do cliente; ii) falsificar relatórios; iii) intencionalmente deixar de cumprir uma etapa do serviço ou realizá-la de forma maliciosa; iv) e trocar objetos em condições ruins por outros que possam ser bem avaliados. Por outro lado, o cliente do organismo de avaliação da conformidade, com o intuito de minimizar ou evitar custos adicionais adventos de possíveis adequações de seu objeto a ser avaliado, também pode realizar ações fraudulentas. Esses clientes podem adulterar o objeto a ser avaliado, falsificar documentos ou tentar subornar a empresa de avaliação da conformidade para receber um certificado de aprovação.

Embora ambos comportamentos fraudulentos sejam perniciosos a saúde e segurança da sociedade, neste trabalho, consideram-se apenas as fraudes realizadas pelos organismos de avaliação da conformidade.

1.4 Motivação

Para monitorar os organismos de avaliação da conformidade acreditados, além das supervisões pré-programadas, a CGCRE realiza, eventualmente, uma visita surpresa a essas organizações. Estas visitas tem o objetivo de verificar se o organismo de avaliação da conformidade está atuando conforme regulamentos técnicos. No entanto, devido ao grande número de empresas acreditadas e do alto custo dessas visitas, não é viável realizar esse procedimento de fiscalização em todas as empresas.

Além disso, em cada organização de avaliação da conformidade, geralmente, não há tempo para analisar todos os registros produzidos pela empresa, devido ao

grande número de serviços realizados, bem como ao volume de dados que devem ser processados. Assim, é imperativo o desenvolvimento de ferramentas que permitam a realização de atividades de fiscalização de empresas de avaliação da conformidade de forma mais eficiente.

1.5 Contribuições

O objetivo desta tese é propor uma sistemática para monitoramento de organismos de avaliação da conformidade a fim de identificar possíveis comportamentos fraudulentos nas execuções de seus serviços. As principais contribuições deste trabalho são:

Contribuição 1: proposta de taxonomia para os tipos de fraudes existentes no âmbito da avaliação da conformidade com relação aos organismos acreditados e seus clientes.

Contribuição 2: proposta de técnicas computacionais para detecção de potenciais serviços fraudulentos, e proposta de modelos matemáticos para simulação de ataques de fraudadores no contexto da avaliação da conformidade.

Contribuição 3: proposta de técnicas para processamento mais eficiente de filmagens de modo a identificar potenciais serviços fraudulentos no âmbito da avaliação da conformidade.

1.6 Organização do texto

Este trabalho está organizado da seguinte maneira: o capítulo 2 mostra trabalhos relacionados, o capítulo 3 apresenta alguns conceitos básicos , por sua vez o

capítulo 4 discorre sobre o arcabouço proposto nesse trabalho; em seguida o capítulo 5 mostra o processo de validação das técnicas que constituem o arcabouço, e por fim, o capítulo 6 apresenta conclusões e trabalhos futuros.

2 TRABALHOS RELACIONADOS

Este capítulo apresenta o processo utilizado para realizar a revisão de literatura deste trabalho. As etapas desse processo foram inspiradas e adaptadas das orientações apresentadas por Kitchenham et al. em (KITCHENHAM et al., 2009).

2.1 Questões de pesquisa

Um organismo de avaliação da conformidade é um prestador de serviços. Desta forma, a revisão de literatura realizada neste trabalho focou fraudes e técnicas para detectar essas fraudes no contexto de prestadores de serviços. Tomou-se como referência as seguintes questões de pesquisa:

Q1 Quais são os tipos de fraudes que ocorrem em prestadores de serviços ?

Q2 Quais são as técnicas computacionais utilizadas na detecção de fraudes em prestadores de serviços?

2.2 Processo de pesquisa

A estratégia de pesquisa denota-se pela identificação das palavras-chave a serem usadas na coleta de trabalhos relevantes e pela coleta desses trabalhos nos bancos eletrônicos de trabalhos científicos. Esse procedimento consiste em dois passos. O primeiro passo denota-se pela construção de palavras-chave. Por sua vez, o segundo passo apoia-se no estabelecimento de uma cadeia de pesquisa usando lógica

booleana e suas aplicação nas ferramentas de pesquisa disponibilizadas nos bancos eletrônicos de trabalhos científicos.

2.2.1 Fontes de pesquisa

Neste trabalho, as fontes de pesquisa utilizadas foram IEEEXplore, SpringerLink, ACM Digital Library, ScienceDirect e NCBI. Essas fontes possuem meios de pesquisa avançada. Elas foram escolhidas, pois permitem a construção de cadeias de pesquisa possibilitando uma investigação dirigida de trabalhos científicos.

A fim de minimizar a coleta de trabalhos não relevantes foram considerados apenas trabalhos entre 2012 e 2017, somente na áreas de Ciência da Computação e Engenharia.

2.2.2 Cadeias de pesquisa

A cadeia de pesquisa é uma forma de mostrar como os termos de pesquisa foram relacionados durante a coleta de trabalhos relevantes nos acervos eletrônicos de trabalhos científicos. O estabelecimento da cadeia de pesquisa vale-se da lógica booleana. Os principais termos utilizados são o AND, OR e NOT.

Para responder as questões de pesquisa, utilizou-se a seguinte cadeia de termos

Fraud **AND** *Detection* **AND** *Service*

2.2.3 Critérios de inclusão e exclusão

A aplicação do método automático de pesquisa retornou um número grande artigos. De modo a selecionar os artigos mais relevantes, estabeleceu-se critérios para inclusão e exclusão de trabalhos. Esses critérios foram:

1. Título e Resumo
2. Introdução - conclusão
3. Texto completo
4. Qualidade do trabalho

A seguir são descritas as etapas do processo de seleção dos artigos.

2.2.4 Critério de título e resumo

Na aplicação desse critério, foi levado em conta a análise do título, resumo e palavras-chave do trabalho coletado. Trabalhos que não apresentavam detecção de fraude foram excluídos. Os trabalhos que continham poucos detalhes no seu resumo foram repassados para próxima etapa.

2.2.5 Critério de introdução-conclusão

Nesta etapa, levou-se em conta a análise da introdução e da conclusão do trabalho. Trabalhos que não apresentavam um problema de fraude no contexto de prestação de algum serviço foram excluídos. Trabalhos que continham poucos

detalhes na introdução sobre o tipo de fraude combatida foram repassados para próxima etapa.

2.2.6 Critério de texto completo

Nesta etapa, levou-se em conta a análise do texto completo do trabalho. Trabalhos que não definiram claramente o tipo de fraude combatida, ou não possuía uma organização realizando fraude em um serviço prestado foram excluídos. Além disso, alguns artigos foram eliminados, pois apresentavam uma nova técnica e a validação dessa técnica não usava casos de fraude.

2.2.7 Critério de qualidade do trabalho

A avaliação da qualidade dos trabalhos coletados foi feita de forma simplificada. Verificou-se apenas se o estudo apresentava objetivos bem definidos, se a modelagem do problema estava bem determinada e se os resultados estavam claramente expressos. Nenhum artigo foi excluído nessa etapa.

2.3 Resultados da pesquisa

O número de trabalhos retornados pela cadeia de pesquisa foi de 2570 trabalhos científicos. Analisando o título e resumo de cada artigo, selecionou-se 127 artigos. Em seguida, analisou-se as informações contidas na Introdução e na Conclusão dos 127 trabalhos restantes. Como consequência da aplicação desse critério foram selecionados 46 artigos. Prosseguindo analisou-se por completo os textos dos 46 artigos remanescentes e a qualidade desses trabalhos, nesse momento foram sele-

cionados 13 trabalhos. Embora não tenham sido retornados pelas bases de pesquisa usando a cadeia de palavras-chave definidas anteriormente, foram incluídos nessa revisão de literatura mais 8 artigos que foram coletados durante o desenvolvimento desta tese. Desta forma, obteve-se um total de 21 trabalhos selecionados para compor a revisão de literatura desta tese.

2.3.1 Tipos de fraudes em prestadores de serviço

Esta seção apresenta os tipos de fraude encontradas no contexto de prestadores de serviço. A Tabela 2.1 mostra uma lista para os tipos de fraudes encontradas nessa revisão de literatura.

Tabela 2.1: Tipos de fraudes encontradas na revisão de literatura

Contexto	Ocorrência
Seguradora	Cláusulas enganosas
Táxi	Rotas desnecessárias
Táxi	Taxímetro adulterado
Supermercado	Não realização de cobrança
Pesquisas por entrevistas	Falsificação de respostas
Ensaios clínicos	Desvios de protocolo
Ensaios clínicos	Falsificação de resultados
Transporte marítimo	Transporte ilegal de produtos
Tratamento médico	Prescrições desnecessárias

2.3.1.1 Fraude em seguradora de veículos

A fraude em seguro de automóvel ocorre quando o vendedor desse produto intencionalmente tenta enganar o consumidor. Isto pode envolver o estabelecimento de cláusulas enganosas nos contratos de seguro ou o não pagamento da indenização estabelecida pelo seguro (JINKA; RAO; SUNDARARAMAN, 2012).

2.3.1.2 Fraude em táxi

As fraudes no serviço de táxi ocorrem quando taxistas cobram preços excessivos pelo serviço prestado, seja por uso de rotas desnecessárias (CHEN et al., 2013), ou por adulteração do taxímetro (LIU; NI; KRISHNAN, 2014).

2.3.1.3 Fraude em caixa de supermercado

A fraude em caixa de supermercado ocorre quando o empregado de modo proposital deixa de computar um determinado produto dando o gratuitamente ao consumidor (TRINH et al., 2011). Esse tipo de fraude também é conhecido como "sweethearting"(doce coração), pois geralmente ocorrem quando os consumidores são parentes do caixa ou são amigos.

2.3.1.4 Fraude em pesquisas por entrevistas

A fraude em pesquisas por entrevista ocorrem quando o entrevistador falsifica os resultadas da pesquisa. Seja por se sentirem desconfortáveis em realizar perguntas sensíveis, ou por receber compensação financeira pelo número de entrevistas realizadas (BIRNBAUM et al., 2013) e (BREDL; WINKER; KÖTSCHAU, 2012).

2.3.1.5 Fraude em ensaios clínicos

A fraude em ensaios clínicos ocorrem quando o laboratório intencionalmente comete desvios no protocolo de ensaio utilizado, ou quando o laboratórios falsificar

os resultados, seja por clonagem de medições realizadas ou por invenção total de medidas (POGUE et al., 2013).

2.3.1.6 Fraude em transporte marítimo

A fraude em transporte marítimo consiste na realização de carregamento e deslocamento de produtos que não atendem as legislações dos países envolvidos na transação dos produtos (CAMOSSI; DIMITROVA; TSOIS, 2012).

2.3.1.7 Fraude em tratamento médico

As fraudes nos tratamentos médicos ocorrem principalmente nas prescrições desnecessárias. Elas são caracterizadas quando o profissional médico prescreve exames, remédios e cirurgias que o paciente não precisa. Muitas vezes favorecendo outros profissionais que são parceiros financeiros do médico que realizou a prescrição (THORNTON et al., 2015), (RASHIDIAN; JOUDAKI; VIAN, 2012).

2.3.2 Técnicas para detecção de fraudes em prestadores de serviço

Nesta seção, são apresentadas as técnicas encontradas nessa revisão de literatura para detecção de fraudes em prestadores de serviço. Essas técnicas podem ser classificadas como sendo técnicas supervisionadas ou não-supervisionadas.

2.3.2.1 Supervisionadas

Para as técnicas supervisionadas, faz-se necessário conhecer o conjunto de dados classificados como fraudulentos e o conjunto de dados classificados como legítimos (ABDALLAH; MAAROF; ZAINAL, 2016). Destacam-se entre as técnicas supervisionadas: redes neurais (JINKA; RAO; SUNDARARAMAN, 2012), (PENG; YOU, 2016); árvores de decisão (JOUDAKI et al., 2014), (ARAL et al., 2012); *k-nearest neighbors*, suporte de vetores, regressão logística (ABDALLAH; MAAROF; ZAINAL, 2016) e algoritmo de florestas aleatórias (BIRNBAUM et al., 2013). A aplicação dessas técnicas exige que o usuário esteja confiante que as classes atribuídas aos dados estão corretas. Isto é necessário para que se possa construir um modelo representativo do tipo classificação a ser realizada. Além disso, essas técnicas só podem ser usadas para classificar elementos que ocorreram previamente.

2.3.2.2 Não-supervisionadas

Já para as técnicas não-supervisionadas, tem-se um conjunto de dados não-rotulados, em que se assume que a maioria dos dados são legítimos (ABDALLAH; MAAROF; ZAINAL, 2016). Destacam-se entre as técnicas não-supervisionadas: agrupamento (LIU; NI; KRISHNAN, 2014), (JOUDAKI et al., 2016), (KOSE; GOKTURK; KILIC, 2015), (TRINH et al., 2011), (BREDL; WINKER; KÖTSCHAU, 2012), regras de associação (ARAL et al., 2012), Lei de Benford (POGUE et al., 2013), (GEORGE; BUYSE, 2015), (HEIN et al., 2012), detecção de valores discrepantes (CHEN et al., 2013), ranque em redes sociais (WANG et al., 2016), análise espectral (CHEN; GANGOPADHYAY, 2013) e classificação de uma classe (CAMOSSI; DIMITROVA; TSOIS, 2012). Essas técnicas podem ser usadas para descobrir novos tipos de classes que não ocorreram previamente.

2.3.2.3 Discussão

Em geral as técnicas supervisionadas têm o benefício de que a saída expressa pelo algoritmo em formato de classes têm significado que pode ser entendido pelos usuários com mais facilidade. Essas técnicas também podem ser usadas para realizar uma regressão com relação aos dados sob estudo. Porém, as técnicas supervisionadas possuem algumas limitações, uma delas é a dificuldade de coletar exemplos rotulados das classes que seja deseja modelar, sem contar que é difícil encontrar dados que são puramente distintos com relação a suas classes, muitas vezes existem incertezas ou ambiguidades com relação ao rótulo atribuído a um determinado conjunto de dados.

Por sua vez, as técnicas não-supervisionadas possuem o benefício de não necessitar de dados precisamente rotulados que muitas vezes são poucos ou inexistentes. Entretanto, essas técnicas se apoiam na premissa que a maioria dos dados sob estudo são de uma determinada classe, caso essa prerrogativa não seja verdadeira, pode-se ter muitos falsos positivos.

A Figura 2.1 mostra o resumo das técnicas levantadas nessa revisão de literatura, bem como seu tipo, vantagens e desvantagens. Para o leitor interessado em conhecer mais tipos de fraude e técnicas que podem ser usadas para detectá-las, recomenda-se consultar o seguintes trabalhos (BEHDAD et al., 2012), (CHANDOLA; BANERJEE; KUMAR, 2009), (HODGE; AUSTIN, 2004), (ALLAN; ZHAN, 2010) e (BOLTON; HAND, 2002).

Técnicas	Tipo	Vantagens	Desvantagens
Árvore de decisão	Supervisionada	Saída de fácil entendimento	Dificuldade em se encontrar dados rotulados
Rede neural			
Máquina de suporte de vetores			
Algoritmo de florestas aleatórias		Podem ser usadas para fazer uma regressão com os dados sob estudo	Podem existir ambiguidades ou incertezas entre classes
K-vizinhos mais próximos			
Regressão logística			
Agrupamento	Não-supervisionada	Não necessitam de dados rotulados	Podem incorrer em muitos falsos positivos
Detecção de valores discrepantes			
Lei de Benford			
Análise espectral			
Ranque em redes sociais			
Regras de associação			
Classificação com uma classe			

Figura 2.1: Resumo das técnicas levantadas nessa revisão de literatura, com seu tipo, vantagens e desvantagens.

Por fim, cabe destacar que analisando a trabalhos na literatura identificou-se propostas de arcabouço com funções semelhantes ao realizado neste trabalho, (DAI et al., 2016) e (WEI et al., 2017). Podem ser destacadas as seguintes funções pré-processamento de dados, aplicação de técnicas de classificação para indicação de instâncias suspeitas, a verificação dessas instâncias para confirmação dos casos de fraude e a criação de históricos de casos de fraude para retroalimentação do sistema.

2.4 Resumo

Neste capítulo, apresentou-se uma revisão de literatura inspirada nos passos de uma revisão sistemática. Através dos trabalhos coletados, construiu-se uma proposta de taxonomia destacando os tipos de fraude que podem ocorrer durante a

prestação de serviços. Além disso, também foram discutidas as técnicas que podem ser usadas para detecção dessas fraudes. No próximo capítulo, serão mostrados os conceitos básicos necessários ao entendimento do arcabouço proposto.

3 CONCEITOS BÁSICOS

Este capítulo descreve os conceitos básicos que dão suporte a esta tese e são importantes para o entendimento do arcabouço proposto. Os elementos utilizados no desenvolvimento deste arcabouço são explicados de acordo com a função proposta no arcabouço.

3.1 Comparando resultados de organismos de avaliação da conformidade

A comparação de organismos de avaliação da conformidade pode permitir um direcionamento quanto as ações de fiscalização do órgão acreditador em seu papel de supervisionar tais organizações. Uma das formas de se realizar tais comparações é utilizando testes estatísticos como o teste de hipótese.

3.1.1 Teste de hipótese

Um teste de hipótese é um procedimento que decide qual de duas afirmações contraditórias sobre uma distribuição estatística é correta. Este procedimento permite avaliar se determinado efeito é real ou ocorreu por acaso (DOWNEY, 2014).

Uma hipótese estatística é uma afirmação sobre o valor de um parâmetro, sobre os valores de vários parâmetros ou sobre a forma de uma distribuição de probabilidade. A hipótese nula, denotada por H_0, é a afirmação que inicialmente assume-se ser verdadeira. A hipótese alternativa, denotada por H_a, é a afirmação que

é contraditória a H_0. A hipótese nula será rejeitada em favor da hipótese alternativa apenas se o caso avaliado possuir evidência de que H_0 é falsa. Se o caso não contradiz fortemente H_0, continuará a crença que a hipótese nula é mais plausível. As duas conclusões possíveis de um teste de hipótese são rejeitar H_0 ou falhar em rejeitar H_0 (ZIEGEL, 2012).

Em um teste de hipótese, o nível de significância α é a probabilidade de se rejeitar a hipótese nula H_0 quando ela é verdadeira. Por sua vez, o valor p é o menor nível de significância que levaria a rejeição da hipótese nula H_0 considerando um determinado conjunto de dados. Para se fazer uma decisão apropriada sobre a rejeição ou não da hipótese nula, tem-se que determinar um valor de corte para o valor p, esse valor de corte é o nível de significância α. Se o valor p é maior que ou igual a α, falha-se ao rejeitar H_0. Por outro lado, se o valor p é menor que α, rejeita-se H_0 (MONTGOMERY; RUNGER, 2010).

O nível de significância α também é conhecido como a probabilidade do erro de tipo I acontecer. O erro de tipo I ocorre quando a hipótese nula é rejeitada, embora ela seja verdadeira. Assim, o erro de tipo I pode ser visto como uma medida de risco, especificamente, o risco de se concluir que a hipótese nula é falsa quando na verdade não é. Portanto, para escolher o valor de α deve-se escolher um valor que reflita as consequências (econômicas, sociais, etc) de se equivocadamente rejeitar a hipótese nula. Pequenos valores refletem sérias consequências, por sua vez, valores maiores refletem consequências menos severas. Uma prática amplamente usada no teste de hipótese é escolher um nível de significância de 0,05 % (MONTGOMERY; RUNGER, 2010).

3.1.2 Método de Bootstrap

Bootstrap é um método computacional que atribui medidas de precisão a estimativas estatísticas (EFRON; TIBSHIRANI, 1994). Este método também pode ser usado como um teste de hipótese. E como em outros testes de hipótese, o primeiro passo é determinar a hipótese nula H_0, a hipótese alternativa H_a e o nível de significância α. Assim, usando o nível de significância, o número de reamostragens η pode ser determinado. Um número η igual a 1000 reamostragens é um valor mínimo razoável para o teste com nível de significância de 5%, enquanto 5000 reamostragens é um valor razoável para um nível de significância de 1% (BRYAN, 2006).

Depois de definir o nível de significância e consequentemente o número de reamostragens, o próximo passo é selecionar aleatoriamente os dados através de um amostragem com reposição e calcular a estatística de interesse S para os dados reamostrados. Após repetir este procedimento η vezes, a distribuição empírica para a estatística de interesse S é construída. O valor s_0 de S para os dados observados é comparado com a distribuição empírica de S. Por exemplo, em um teste unilateral, onde é requerido decidir se um parâmetro é maior que um determinado valor, se s_0 se apresentar como um valor típico na distribuição empírica de S, aceita-se a hipótese nula. Caso contrário, se s_0 é um valor incomum e alto, então os dados não apresentam evidência de que a hipótese nula é verdadeira, assim pode-se concluir que a hipótese alternativa é mais plausível. O nível de significância de s_0 é a proporção ou porcentagem dos valores que são maiores ou iguais a s_0 na distribuição empírica de S (BRYAN, 2006). A Figura 3.1 ilustra a aplicação do método de Bootstrap.

No trabalho de Taylor *et al*, os autores propuseram uma técnica para identificar questionários falsificados utilizando um método gráfico e o método de Bootstrap. O método proposto explorou a estrutura de correlação de um questionário e a dificuldade de se fabricar tais detalhes (TAYLOR; MCENTEGART; STILLMAN, 2002).

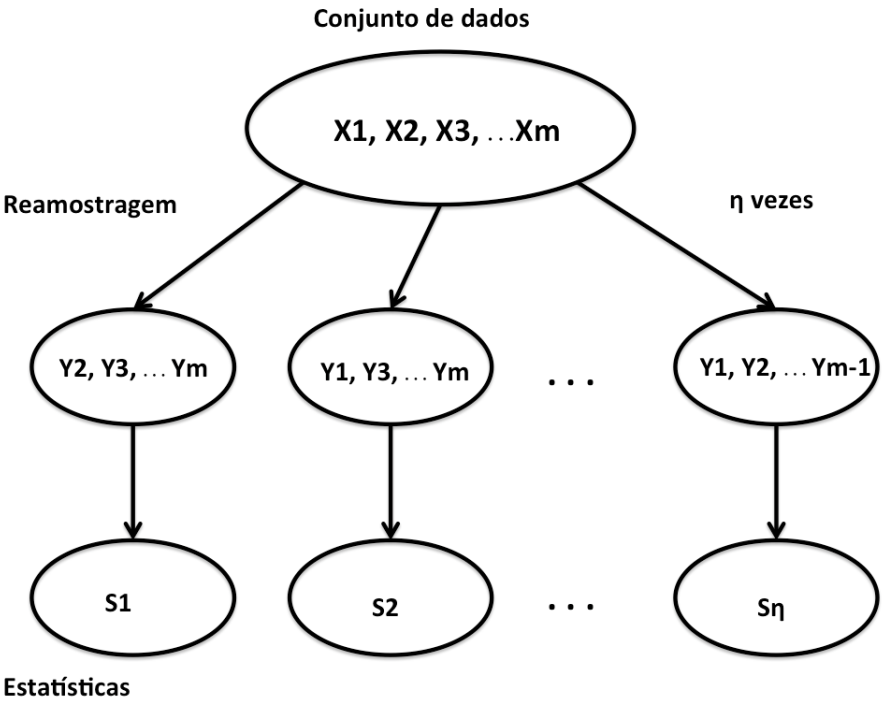


Figura 3.1: Ilustração do processo do método de Bootstrap.

Além disso, o método de Bootstrap foi utilizado na criação de conjunto de dados sintéticos para validação da metodologia de detecção de entrevistas falsificadas em (HAAS; WINKER, 2016).

3.1.3 Teoria de Dempster-Shafer

A teoria de Dempster-Shafer é uma teoria matemática baseada em duas ideias. A primeira é a noção de graus de crença para uma questão apoiada em probabilidades subjetivas. A segunda é a regra de Dempster para combinação de graus de crença de itens independentes de evidência (SHAFER et al., 1976).

Na teoria de Dempster-Shafer, o conjunto de todos os possíveis estados que um sistema pode assumir é chamado de conjunto de discernimento denotado por Ω, que é similar ao espaço de estados em probabilidade. As hipóteses na teoria de Dempster-Shafer referem-se a todos os possíveis subconjuntos do conjunto de discernimento. O grupo de todos os possíveis subconjuntos de Ω, incluindo ele mesmo e o conjunto vazio, é denotado por 2^{Ω} (YONG et al., 2011).

Os elementos de 2^{Ω} podem ser hipóteses simples ou um conjunto de hipóteses. Além disso, na teoria de Dempster-Shafer é requerido que as hipóteses sejam únicas, que não haja interseção entre elas e que sejam mutuamente exclusivas. Neste contexto, as evidências são sintomas ou eventos que ocorrem ou podem ocorrer no sistema. Uma evidência é relacionada a uma hipótese simples ou a um conjunto de hipóteses. Fontes de evidência são pessoas, organizações, ou qualquer outras entidades que forneçam informação para um cenário (KAY, 2007).

Através das fontes de evidência, a função de mapeamento $m : 2^{\Omega} \rightarrow [0, 1]$ atribui um peso de evidência a um subconjunto em Ω que contém um única hipótese

ou um conjunto de hipóteses. Esta função m é chamada atribuição de probabilidade básica. A função m é o grau de crença que um afirmação especificada é assegurada (KAY, 2007). Tendo o conjunto de todos os estados possíveis, para uma determinada hipótese H tem-se

$$\begin{cases} m(\emptyset) = 0 \\ m(H) \geq 0, \forall H \in 2^{\Omega} \\ \sum_{H \in 2^{\Omega}} m_1(H) = 1 \end{cases} \tag{3.1}$$

Aplicando a função de atribuição de probabilidade básica, muitas funções de evidência podem ser criadas. A medida de crença é dada por $Bel : 2^{\Omega} \rightarrow [0, 1]$. A função de crença pode ser interpretada como o total de suporte dado a um subconjunto em Ω. Para combinar duas evidências independentes, pode-se usar a regra de Dempster expressa pela equação

$$Bel(Z) = \frac{\sum_{A \cap B = Z} m_1(A) m_2(B)}{1 - \sum_{A \cap B = \emptyset} m_1(A) m_2(B)} \tag{3.2}$$

com A, B, Z $\subseteq \Omega$ e as funções de atribuição de probabilidade básica m_1 and m_2. Em outras palavras, o numerador representa a evidência acumulada para os conjuntos A e B, que dão suporte a hipótese Z, e o denominador quantifica a quantidade de conflito entre os dois conjuntos A e B (KAY, 2007).

No trabalho de Yong *et al*, apresenta-se a utilização da teoria de Dempster-Shafer na detecção de fraudes em serviços de táxi. Essa técnica calcula o grau de anomalia do serviço prestado pelo taxista combinando, através da teoria de Dempster-Shafer, duas evidências: rota traçada e a distância percorrida (YONG et al., 2011). Há também a aplicação da teoria de Dempster-Shfaer no método híbrido estabelecido para detecção de fraudes em planos de saúde (SUN et al., 2016).

3.2 Selecionando possíveis serviços fraudulentos de organismo de avaliação da conformidade

A análise dos resultados dos serviços de um organismo de avaliação da conformidade pode levar a detecção de anomalias como execução de serviços fraudulentos. Esse tipo de análise pode se apoiar em técnicas de aprendizado de máquina, bem como em procedimentos estatísticos. Neste caso, o principal objetivo seria apontar os serviços com maior chance de serem fraudulentos.

3.2.1 Redes Neurais - *Learning Vector Quantization*

As redes neurais são usualmente aplicadas para reconhecimento de padrões estatísticos, em que as classes de distribuições de vetores padrões costumam se sobrepor e onde se deve procurar as fronteiras ótimas para tomada de decisão. O algoritmo de *Learning Vector Quantization* - (LVQ) é adequado para esse tipo de situação e também é computacionalmente leve (ARBIB, 2003).

O LVQ utiliza regras de aprendizado competitivo. Para cada padrão de entrada, os neurônios da grade calculam seus respectivos valores através de uma função discriminante. Esta função discriminante fornece a base para a competição entre os neurônios. O neurônio particular com o maior valor da função discriminante é declarado vencedor da competição.

3.2.2 Lei de Benford

Segundo a Lei de Benford, em alguns conjuntos de dados, a frequência de aparição dos dígitos mais significativos segue uma distribuição logarítmica (NIGRINI,

2012). As Equações 3.3 e 3.4 apresentam as fórmulas das probabilidades esperadas para o primeiro e para o segundo dígito mais significativo respectivamente:

$$P(D_1 = d_1) = \log\left(1 + \frac{1}{d_1}\right) \tag{3.3}$$

$$P(D_2 = d_2) = \sum_{d_1=1}^{9} \log\left(1 + \frac{1}{d_1 d_2}\right) \tag{3.4}$$

onde P indica a probabilidade de se observar o evento entre parênteses, D_1 e D_2 representam o primeiro e o segundo dígito mais significativo de um número $D_1 \in \{1, 2, 3, ...9\}$ and $D_2 \in \{0, 1, 2, 3, ..., 9\}$.

Por sua vez, a Equação 3.5 apresenta a fórmula das probabilidades esperadas para os dois primeiros dígitos mais significativos:

$$P(D_1 D_2 = d_1 d_2) = \log\left(1 + \frac{1}{d_1 d_2}\right) \tag{3.5}$$

onde $D_1 D_2$ representa os dois primeiros dígitos mais significativos, $d_1 d_2 \in \{10, 11, 12, 13, ..., 99\}$.

Segundo (NIGRINI, 2012), a Lei de Benford só pode ser aplicada a uma conjunto de dados se as seguintes condições forem satisfeitas: i) os dados dessa conjunto devem conter informação de tamanho de fatos ou eventos. Por exemplo, tamanho de cidades, vazão de rios e lucro de empresas; ii) o conjunto não deve possuir mínimos e máximos embutidos, exemplo: um fundo de investimento com valor mínimo de R$500,00 de aplicação; iii) os elementos do conjunto não podem ser

dados de identificação, como número de telefone e placas de veículos; iv) a média dos dados deve ser menor que a mediana e os dados não devem ficar fortemente agrupados em torno do valor médio.

Algumas distribuições estatísticas como a exponencial, gama e log-normal atendem a Lei de Benford de forma aproximada (FORMANN, 2010). Por fim, para se aplicar a Lei de Benford o conjunto de dados deve ser grande o suficiente. Sabe-se que para alguns conjuntos de dados com 50 a 100 números a Lei de Benford apresentou-se eficaz, no entanto, alguns especialistas indicam que um conjunto de dados com 500 ou mais elementos é mais indicado para aplicação dessa lei (COLLINS, 2017).

A Lei de Benford tem sido aplicada em alguns trabalhos sobre detecção de fraudes, como por exemplo, em (BARABESI et al., 2017) os autores aplicam a Lei de Benford na detecção de fraudes em transações comerciais internacionais. Por sua vez, em (HÜLLEMANN; SCHÜPFER; MAUCH, 2017), os autores utilizam a Lei de Benford na detecção de artigos científicos fraudulentos.

3.2.3 Processos de Decisão de Markov

Um Processo de Decisão de Markov é uma tupla (S, A, T, R) onde: S é o conjunto de estados , A é o conjunto de ações , $T : S \times A \times S \rightarrow [0, 1]$ é uma função de probabilidade de transição do estado $s \in S$ para $s\prime \in S$, dado uma ação $a \in A$ (denotada por $T(s\prime \mid s, a)$) e $R : S \times A \rightarrow \mathbb{R}$ é uma função que dá o custo (ou recompensa) quando o agente está no estado $s \in S$ toma uma decisão $a \in A$ e vai para o estado $s\prime \in S$ (denotada por $R(s\prime \mid s, a)$) (DAVID; ALAN, 2010). O nome Markov se deve a propriedade Markoviana (sem memória), isto é a definição do próximo estado do agente só depende do estado atual. Uma política π é uma

função que mapeia estados em ações, sendo que o objetivo do Processo de Decisão de Markov é encontrar uma política que maximize sua recompensa acumulada ao longo prazo. Uma forma de se medir o desempenho do agente num MDP é usando o critério de recompensa esperada descontada $E\left[\sum_{k=0}^{\infty}\gamma^k r_k\right]$, onde r_k é a recompensa no passo k e γ é o fator de desconto, que é usado para garantir a convergência do valor da recompensa total esperada.

Em economia, γ pode ser visualizado como uma taxa de juro. Já de um ponto de vista de probabilidade, o fator γ pode ser visto como a probabilidade do agente sobreviver no ambiente de exploração (DAVID; ALAN, 2010).

A função $V^{\pi}(s)$ é o valor esperado da recompensa descontada para o agente que sai do estado s e segue a política π. Já a função $Q^{\pi}(s,a)$ é o valor da recompensa esperada descontada quando o agente sai do estado s escolhendo a ação a e seguindo a política π. A função de valor $V^*(s)$ ótima é definida como $V^*(s) = \max_{\pi}(V(s))$ para todo $s \in S$. Valendo também $V^*(s) = \max_{a}(Q^*(s,a))$ e $\pi^* = \arg\max_{a}(Q^*(s,a))$. Existe uma grande quantidade de algoritmos para a solução de um MDP. Alguns trabalham diretamente com políticas, enquanto outros trabalham com funções valor, detalhes sobre esses algoritmos podem ser encontrados em (DAVID; ALAN, 2010).

3.2.4 Mineração de Dados

A Mineração de Dados consiste na extração de conhecimento de uma massa de dados disponível (PAOLO, 2003). O processo de Mineração de Dados geralmente segue as seguintes etapas: Definição dos Objetivos, Limpeza de Dados, Integração de Dados, Seleção de Dados, Transformação de Dados, Mineração de Dados e Representação do Conhecimento (LAKSHMI; RAGHUNANDHAN, 2011). Primeiro passo para aplicação das técnicas de mineração de dados é determinar o que se quer

obter com o estudo. Em seguida, realiza-se a limpeza de dados, onde ruídos e dados irrelevantes são retirados do banco de dados. Depois, decide-se quais são os dados relevantes ao estudo em questão. Caso necessário, os dados selecionados são transformados de modo a serem adequados à técnica de Mineração de Dados que será utilizada. Por fim, as técnicas de Mineração de Dados são empregadas para extrair padrões potencialmente úteis e o conhecimento extraído é visualizado e interpretado pelo usuário.

3.2.5 Detecção de anomalias

Deteccão de anomalia se refere ao problema de encontrar padrões em um conjunto de dados que não estão conformes a um comportamento esperado. Um aspecto importante nesse processo é a maneira em que as anomalias são reportadas. Um tipo de saída que uma técnica de detecção de anomalia pode produzir é uma função de pontuação. Esta função atribui um grau de anomalia a cada elemento no conjunto de dados testados. Consequentemente, a saída dessa função é uma lista com o ranking dos elementos anômalos. Um analista pode escolher entre analisar um subconjunto dos elementos anômalos ou usar um limiar de corte para selecionar os elementos anômalos (CHANDOLA; BANERJEE; KUMAR, 2009).

Técnicas de Mineração de dados e de detecção de anomalias podem ser utilizadas na detecção de fraudes em pedágios (ZHIJUN; CHUANGWEN, 2009), roubo de energia elétrica (ANGELOS et al., 2011) e na deteção de phishing (ZHUANG et al., 2012). Há também o emprego de técnicas de mineração de dados na deteção de fraudes em planos de saúde (GHUSE; PAWAR; POTGANTWAR, 2017) e transações financeiras (BARMAN et al., 2016).

3.3 Analisando os serviços de avaliação da conformidade através de filmagens

O recente crescimento da utilização de sistemas de vigilância através de câmeras de vídeo tem permitido a realização de diversas aplicações como detecção de comportamentos anômalos em multidões, bem como, deteção de fraude em atividades de supermercado. No contexto de avaliação da conformidade, também pode-se utilizar sistemas de vigilância por vídeo para verificar se uma determinada organização está atuando conforme os regulamentos técnicos estabelecidos para suas atividades. Uma das formas de se iniciar tal monitoramento é através da detecção das movimentações dentro do organismo de avaliação da conformidade.

3.3.1 Detecção de movimentos

Detecção de movimento é o processo de analisar sucessivos quadros de um vídeo para identificar objetos que estejam em movimento. A habilidade de estimar, analisar e compensar por movimentos relativos é um requisito comum em muitos algoritmos de processamento de vídeos (MARQUES, 2011).

Uma maneira simples de detectar movimento em uma sequência de imagens consiste em usar uma técnica chamada Diferença Temporal (LIPTON; FUJIYOSHI; PATIL, 1998). Esta técnica faz uso da diferença entre dois ou três quadros consecutivos em uma sequência de imagens para extrair regiões de movimento. Se I_n é a intensidade do n-ésimo quadro, então a função diferença D_n é

$$D_n = |I_n - I_{n-1}| \tag{3.6}$$

Após a diferença absoluta entre dois quadros consecutivos ser obtida, um função limiar é usada para determinar mudanças. Uma imagem de movimento M_n pode ser extraída através da operação

$$M_n(u,v) = \begin{cases} I_n(u,v),\ D_n(u,v) \geq T \\ 0,\ D_n(u,v) < T \end{cases} \tag{3.7}$$

onde u e v são as coordenadas do pixel na imagem e T é um valor de limiar. O valor de limiar T pode ser determinado empiricamente.

Fatores desfavoráveis ao processo de detecção de movimentos são variação da iluminação, sombras, ramos balançando e mudanças climáticas (HU et al., 2004), (YILMAZ; JAVED; SHAH, 2006), (KIM et al., 2010). Em um organismo de avaliação da conformidade acreditado, geralmente, tem-se ambientes protegidos de mudanças climáticas. Nesse ambiente, o principal elemento que pode afetar o processo de detecção de movimentos é a variação de iluminação, que pode causar falsos positivos na detecção de movimentos.

3.3.2 Filtros homomórficos

Para eliminar a influência indesejável da variação de iluminação durante o processo de detecção de movimento, a componente de reflectância obtida pelo filtro homomórfico pode ser usada (TOTH; AACH; METZLER, 2000), (RADKE et al., 2005). Uma imagem pode ser expressada como o produto de uma componente de iluminação e uma componente de reflectância. Um filtro homomófico pode operar nessas duas componentes separadamente (GONZALEZ; WOODS, 2002).

A intensidade de uma imagem é gerada por uma iluminação incidente, que é

refletida pela superfície dos objetos na cena observada. Considerando um objeto de superfície Lambertiana, pode-se modelar a intensidade do n-ésimo quadro em uma sequência de imagens por

$$I_n(u, v) = i_n(u, v)r_n(u, v) \tag{3.8}$$

onde i é a componente de iluminação e r é a componente de reflectância (OPPENHEIM; SCHAFER; STOCKHAM, 1968). Consequentemente, pode-se extrair a componente de reflectância aplicando-se, primeiramente, o logaritmo e então aplicando-se um filtro passa-baixa. O logaritmo transforma a relação multiplicativa de I, i e r, em uma relação aditiva, isto é,

$$\log(I_n(u, v)) = \log(i_n(u, v)) + \log(r_n(u, v)) \tag{3.9}$$

Figura 3.2 ilustra a estrutura do filtro homomórfico para extrair as componentes de reflectância e iluminação. Depois de aplicar o logaritmo, um filtro passa-baixa é aplicado na imagem e então subtrai-se o logaritmo original, obtendo-se uma componente de um filtro passa-alta. Fazendo a exponenciação das componentes do filtro passa-baixa e passa-alta, tem-se, aproximadamente, as componentes de iluminação e de reflectância de uma imagem (TOTH; AACH; METZLER, 2000).

3.3.3 Kolmogorov-Smirnov teste para duas amostras

O teste de Kolmogorov-Smirnov para duas amostras é um teste para identificar se duas amostras vieram de uma mesma distribuição. Este teste pode ser utilizado para descartar quadros de um vídeo que sejam estatisticamente similares.

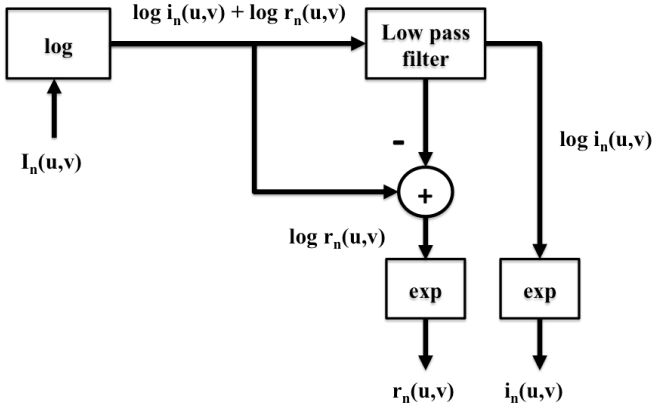


Figura 3.2: Ilustração da estrutura do filtro homomórfico para extrair as componentes de reflectância e iluminação de uma imagem

No caso, pode-se obter esse julgamento usando o teste de Kolmogorov-Smirnov para duas amostras entre os dois histogramas normalizados desses quadros na escala de cinza. Uma característica interessante deste teste, que permite essa aplicação, é que essa técnica não presume a condição dos dados seguirem algum tipo de distribuição específica, como por exemplo a distribuição normal.

Para aplicar o teste de Kolmogorov-Smirnov para duas amostras, uma distribuição acumulada é feita para cada amostra usando-se os mesmos intervalos para ambas as distribuições. Para cada intervalo, uma distribuição acumulada é subtraída da outra. O teste foca na maior diferença entre essas duas distribuições (SIEGEL, 1956).

O valor crítico para a estatística do teste de Kolmogorov-Smirnov é

$$KS = 1,36\sqrt{\frac{n_1 + n_2}{n_1 n_2}} \tag{3.10}$$

onde 1,36 é a constante que corresponde ao nível de significância de 5% e n_1 e n_2 são os números de elementos em cada amostra.

Dentre as aplicações que usa sistemas de vigilância por câmeras para detecção de possíveis ações fraudulentas, pode-se destacar o trabalho de Trinh *et al*, onde técnicas de processamento de imagem são utilizadas para detecção de fraudes em supermercados. Essas técnicas são utilizadas para identificar movimentações maliciosas dos caixas do supermercado no momento da contabilização dos produtos que o cliente deve pagar (TRINH et al., 2011). Além disso, existem aplicações que utilizam sistema de vigilância por vídeos para identificar atividades criminosas em caixas eletrônicos de bancos, como por exemplo (MANDAL; CHOUDHURY, 2016).

3.4 Investigando os serviços de avaliação da conformidade através de retroalimentação

Uma vez que se tenha comprovado quais são os serviços legítimos e os serviços fraudulentos, pode-se utilizar esses elementos para a investigação de casos similares dentro de um conjunto de dados ainda não explorado. Um analista pode optar por realizar a modelagem dos elementos fraudulentos e pesquisar casos parecidos. Ou, alternativamente, ele pode modelar os elementos legítimos e identificar as instâncias que tenham um desvio acentuado do comportamento legítimo modelado. Uma possibilidade para esse tipo de abordagem pode ser a utilização das filmagens dos serviços de avaliação da conformidade para o reconhecimento de ações legítimas ou fraudulentas em outros serviços previamente registrados em vídeo.

3.4.1 Reconhecimento de ações em vídeos

O reconhecimento de ações humanas em vídeos é uma linha de pesquisa bastante ativa na área de visão computacional. Algumas aplicações importantes podem ser vislumbradas nesse segmento, por exemplo, vigilância inteligente, análise de desempenho de atletas e armazenamento e busca de conteúdo em um conjunto de vídeos (WANG; HU; TAN, 2003).

O entendimento de um conjunto de ações pode ser interpretado como a classificação ao longo do tempo de um conjunto de características. Em outras palavras, associar uma sequência de desconhecida com um grupo de sequências que representam um determinado comportamento. Desta forma, o ponto-chave é aprender a uma sequência de referência de um conjunto de dados de treinamento, e estabelecer métodos de treinamento e classificação capazes de tratar as variações no conjunto de características dentro de uma determinada classe (HU et al., 2004).

3.4.2 Fluxo ótico

O fluxo ótico pode ser tratado como uma movimentação aparente de objetos, padrões de brilho, ou outros pontos característicos, observados pelo olho ou por uma câmera. O fluxo ótico pode ser calculado do movimento de objetos com mesmo brilho ou padrão característico entre duas imagens subsequentes (CHAO; GU; NAPOLITANO, 2014).

A maioria dos algoritmos usados no cálculo do fluxo ótico se baseiam em algumas premissas:

a) brilho constante: apenas o movimento do objeto com relação a câmera pode

causar mudanças locais na intensidade da imagem;

b) suavidade espacial: o movimento é uniforme sobre uma pequena vizinhança de pixels na imagem;

c) movimentos pequenos: a frequência de amostragem é rápida o suficiente para representar os movimentos na imagem de forma graudual no tempo.

Matematicamente, pode-se representar essas premissas através da seguintes equações:

$$I(u, v, t) = I(u + \delta u, v + \delta v, t + \delta t) \tag{3.11}$$

$$I_u \dot{u} + I_v \dot{v} + I_t = 0 \tag{3.12}$$

onde $I(u, v, t)$ é a intensidade da luz no ponto (u, v) na imagem plana no tempo t (CHAO; GU; NAPOLITANO, 2014).

3.4.3 Histograma orientado de fluxo ótico

Na literatura de reconhecimento de ações, um dos descritores utilizados é o Histograma orientado de fluxo ótico. Este descritor estabelece a distribuição do fluxo ótico levando em conta a direção e a magnitude dos vetores que representam esse fluxo.

Para estabelecer o Histograma orientado de fluxo ótico, primeiramente calcula-se o fluxo ótico em uma determinada cena. Cada vetor de fluxo é contabilizado de

acordo com seu ângulo em relação ao eixo horizontal do plano da imagem e sua contribuição para o histograma é medida de acordo com a magnitude do vetor. Assim, todo o vetor de fluxo $w = [x, y]^T$ com direção $\theta = \arctan(\frac{x}{y})$ no intervalo $\frac{-\pi}{2} + \frac{\pi(b-1)}{B} \leq \theta < \frac{-\pi}{2} + \frac{\pi(b)}{B}$ irá contribuir com $\sqrt{x^2 + y^2}$ para a soma no intervalo b, $1 \leq b \leq B$, de um total de B intervalos. Por fim, o histograma é normalizado de modo que a somatória seja 1 (CHAUDHRY et al., 2009).

O Histograma orientado de fluxo ótico é independente da direção do movimento. Além disso, a normalização do histograma faz com que ele possua invariância com relação a escala. Assim, espera-se que se observe um mesmo histograma para uma pessoa correndo da esquerda para direita, ou na direção contrária. Bem como, se a pessoa está correndo à distância na cena, ou se está próxima a câmera. Por fim, como a contribuição de cada intervalo no histograma é correspondente a magnitude dos vetores de fluxo, pequenos ruídos tem pouco efeito no histograma observado (CHAUDHRY et al., 2009).

3.4.4 Alinhamento de sequência

O alinhamento de sequência tem por objetivo estabelecer a melhor correspondência entre sequências avaliadas. Dois algoritmos básicos são o de alinhamento global Needleman-Wunsch (NEEDLEMAN; WUNSCH, 1970) e o de alinhamento local Smith-Waterman (SMITH; WATERMAN, 1981).

O alinhamento global é um arranjo de sequências em que todos os elementos em ambas as sequências participam do alinhamento. Por sua vez, o alinhamento local é um método que encontra regiões dentro das sequências que tenham maior similaridade. O alinhamento global é efetivo quando se tem duas sequências de tamanhos similares e homogêneas. De outro lado, para sequências de tamanhos

diferentes e sem homogeneidade, o alinhamento local seria mais indicado (KUNDU; SURAL; MAJUMDAR, 2006).

3.4.4.1 Alinhamento global

O processo de alinhamento de duas sequências com símbolos de um mesmo alfabeto consiste em consecutivamente selecionar cada símbolo ou inserir uma lacuna na primeira sequência e corresponder esse símbolo em particular ou lacuna com outro símbolo na outra sequência (DEONIER; TAVARÉ; WATERMAN, 2005). O processo de alinhamento pode ser representado por uma matriz.

A Figura 3.3 mostra um exemplo hipotético do alinhamento entre duas sequências $S_1 = (a, b, b, c)$ e $S_2 = (a, b, b)$. Um seta horizontal significa que uma lacuna foi inserida em correspondência ao elemento pertencente a sequência representada na parte superior da matriz, enquanto uma seta vertical significa que uma lacuna foi inserida em correspondência ao elemento pertencente a sequência representada na parte esquerda da matriz. Um seta diagonal significa que os elementos são correspondentes, neste caso tem-se uma identidade. Caso os elementos fossem diferentes, ter-se-ia uma não correspondência. O símbolo "-" representa uma lacuna. Qualquer alinhamento é representado por um caminho único através da matriz. A qualidade do alinhamento é medida por um índice de pontuação SP, que é tão maior quanto maior for o grau de similaridade entre as duas sequências que estão sendo alinhadas.

Para o alinhamento global, de acordo com o algoritmo de Needleman-Wunsch (NEEDLEMAN; WUNSCH, 1970), o melhor alinhamento entre as posições i e j em uma matriz de alinhamento é dado por

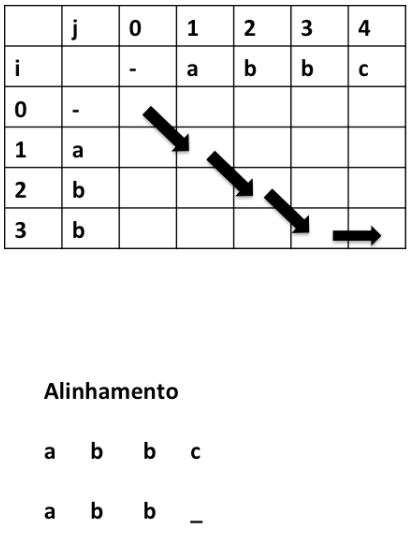


Figura 3.3: Ilustração do processo de alinhamento entre duas sequências.

$$SP_{i,j} = max \left\{ \begin{array}{l} SP_{i-1,j-1} + s(i,j) \\ SP_{i-1,j} + \delta_l \\ SP_{i,j-1} + \delta_l \end{array} \right\} \tag{3.13}$$

onde $s(i,j)$ é a pontuação por se ter uma correspondência ou uma não-correspondência na posição (i,j) e δ_l é a pontuação por se inserir uma lacuna.

Para se preencher a matriz de alinhamento com suas respectivas pontuações, a primeira linha da matriz e a primeira coluna devem ser completadas com $SP_{i,0} = i\delta_l$ e $SP_{0,j} = j\delta_l$. Quando se tem duas sequências A e B com tamanhos n e m respectivamente, a melhor pontuação de alinhamento é dada por $SP_{n,m}$ e se encontra na posição (n,m) da matriz de alinhamento. A foram como as sequências são alinhadas é obtida pelo caminho de volta da matriz seguindo elemento por elemento com pontuação máxima a partir da posição (n,m).

Figura 3.4: Ilustração do processo de alinhamento global entre duas sequências.

Para exemplificar o estabelecimento da pontuação de alinhamento global, tome-se o seguinte exemplo de alinhamento entre as sequências $S_1 = (b, a, c, d)$ e $S_2 = (a, d, e)$, com o seguinte sistema de pontuação, caso haja correspondência na posição (i, j) atribui-se $s(i, j) = 1$, caso haja uma não correspondência na posição (i, j) atribui-se $s(i, j) = -1$ e caso seja inserido uma lacuna atribui-se $\delta_l = -1$. A Figura 3.4 ilustra o exemplo de processo de alinhamento global. As setas pretas mostram o caminho de volta e como seria a forma do alinhamento obtido. Nota-se que a pontuação do alinhamento obtido é $SP_{3,4} = 2$.

3.4.4.2 Alinhamento local

Conforme mencionado anteriormente, o alinhamento local é um método que encontra regiões dentro das sequências que tenham maior similaridade. Segundo o algoritmo de alinhamento local Smith-Waterman (SMITH; WATERMAN, 1981) o melhor alinhamento entre as posições i e j em uma matriz de alinhamento é dado por

$$SP_{i,j} = max \left\{ \begin{array}{l} SP_{i-1,j-1} + s(i,j) \\ SP_{i-1,j} + \delta_l \\ SP_{i,j-1} + \delta_l \\ 0 \end{array} \right\} \tag{3.14}$$

onde $s(i,j)$ é a pontuação por se ter uma correspondência ou uma não-correspondência na posição (i,j) e δ_l é a pontuação por se inserir uma lacuna.

Para exemplificar o estabelecimento da pontuação de alinhamento global, tome-se o seguinte exemplo de alinhamento entre as sequências $S_1 = (a,b,b,c)$ e $S_2 = (a,b,b)$, com o seguinte sistema de pontuação, caso haja correspondência na posição (i,j) atribui-se $s(i,j) = 1$, caso haja uma não correspondência na posição (i,j) atribui-se $s(i,j) = -1$ e caso seja inserido uma lacuna atribui-se $\delta_l = -1$. A Figura 3.4 ilustra o exemplo de processo de alinhamento local. As setas pretas mostram o caminho de volta e como seria a forma do alinhamento obtido. Diferentemente do alinhamento global, o caminho de volta para se obter a forma da região alinha começa no posição de maior pontuação e segue elemento a elemento sempre escolhendo o ponto de máximo valor até atingir alguma posição com pontuação zero. Nota-se que a pontuação do alinhamento obtido é $SP_{3,3} = 3$.

No artigo (KUNDU et al., 2009), os autores empregam técnicas de alinha-

	j	0	1	2	3	4
i		-	a	b	b	c
0	-	0	-1	-2	-3	-4
1	a	-1				
2	b	-2				
3	b	-3				

Passo 1 – Preenche primeiras linha e coluna

	j	0	1	2	3	4
i		-	a	b	b	c
0	-	0	-1	-2	-3	-4
1	a	-1	1	0	0	0
2	b	-2				
3	b	-3				

Passo 2 – Preenche segunda linha

	j	0	1	2	3	4
i		-	a	b	b	c
0	-	0	-1	-2	-3	-4
1	a	-1	1	0	0	0
2	b	-2	0	2	1	0
3	b	-3				

Passo 3 – Preenche terceira linha

	j	0	1	2	3	4
i		-	a	b	b	c
0	-	0	-1	-2	-3	-4
1	a	-1	1	0	0	0
2	b	-2	0	2	1	0
3	b	-3	0	1	3	2

Passo 4 – Preenche quarta linha

Figura 3.5: Ilustração do processo de alinhamento local entre duas sequências.

mento de sequência para detecção de transações fraudulentas no uso de cartão de crédito. No primeiro estágio do sistema proposto, sequências de novas transações são comparadas com sequências de transações passadas genuínas usando técnicas de alinhamento de sequência. Depois, as sequências suspeitas são comparadas com transações fraudulentas. A decisão final sobre a legitimidade da nova sequência de transações é tomada usando as duas comparações anteriores.

3.5 Resumo

Neste capítulo, foram apresentados conceitos básicos que são importantes para o entendimento desta tese. O uso de método de Bootstrap como um teste de hipótese foi destacado, bem como o uso da teoria de Dempster-Shafer para combinar evidências. Também, destacou-se a utilização da Lei de Benford para a detecção de valores discrepantes. Além disso, foram mostrados conceitos sobre processamento de imagens que podem ser utilizados na detecção de anomalias. Bem como, apresentou-se conceitos sobre alinhamento de sequências. No próximo capítulo, o arcabouço proposto será apresentado em detalhes.

4 ARCABOUÇO PARA DETECÇÃO DE POSSÍVEIS SERVIÇOS FRAUDULENTOS EM ORGANISMOS DE AVALIAÇÃO DA CONFORMIDADE

Neste capítulo, apresenta-se uma proposta de um arcabouço para monitoramento de organismos de avaliação da conformidade. O objetivo desse sistema é identificar possíveis comportamentos fraudulentos nas operações dessas organizações. Esse arcabouço é composto pelos seguintes módulos: (i) Análise de organismos de avaliação da conformidade; (ii) Análise dos serviços de avaliação da conformidade; (iii) Análise das filmagens dos serviços realizados; e (iv) Investigação automática de casos similares. A Figura 4.1 ilustra a sistemática proposta.

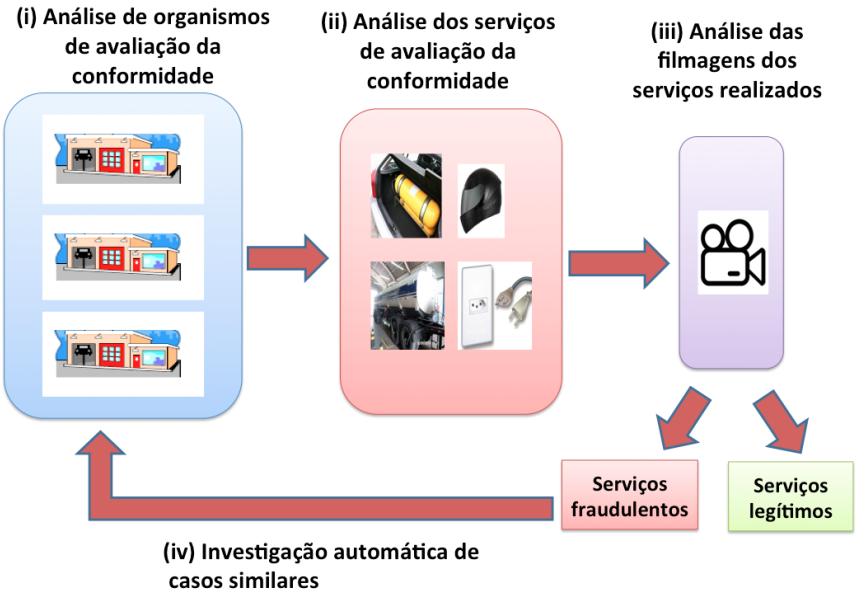


Figura 4.1: Ilustração da sistemática proposta para deteção de possíveis serviços fraudulentos em organismos de avaliação da conformidade.

O módulo de análise de organismos de avaliação da conformidade é responsável por fazer uma comparação entre resultados de organismos congêneres para verificar qual deles é potencialmente fraudulento. Por sua vez, o módulo de análise dos serviços de avaliação da conformidade é responsável por investigar quais serviços de um organismo anômalo tem maior suspeita de conter possíveis fraudes. Ainda, o módulo de análise das filmagens dos serviços realizados tem a função de verificar os registros de filmagens desses serviços para identificar os casos com suspeita de fraude. Por fim, através de modelos de assinatura, o módulo de investigação automática de casos similares tem a incumbência de verificar em organismos congêneres casos de fraude semelhantes

4.1 Análise de organismos de avaliação da conformidade

Tendo em vista o aumento do número de organismos de avaliação da conformidade a cada ano, faz-se necessária uma metodologia para selecionar possíveis organizações com comportamento fraudulento, a fim de otimizar o trabalho do órgão acreditador. Assim, nesta seção, apresenta-se uma proposta de método para detectar organismos de avaliação da conformidade que tenham possíveis resultados com casos de fraude (SOUZA; CARMO; PIRMEZ, 2017).

4.1.1 Detecção de organismos de avaliação da conformidade com possíveis serviços fraudulentos

Para detectar possíveis organismos com comportamento fraudulento, propõe-se um procedimento que emprega o método de Bootstrap com a teoria de Dempster-Shafer. Deseja-se testar se algum organismo de avaliação da conformidade realizou serviços de forma legítima ou de forma potencialmente fraudulenta. O método de

Bootstrap é utilizado pois permite realizar comparação entre dois ou mais conjuntos de dados. Sem contar que essa técnica não requer nenhuma suposição sobre a distribuição estatística dos dados, e também permite a utilização de estatísticas não-convencionais (BRYAN, 2006). Por sua vez, a teoria de Dempster-Shafer permite a fusão de vários aspectos de um comportamento fraudulento em um único grau de anomalia. Além disso, a teoria de Dempster-Shafer leva em conta probabilidades subjetivas sobre uma determinada questão, o que possibilita a incorporação conhecimentos específicos de uma analista (YONG et al., 2011).

Na utilização do o método de Bootstrap com a teoria de Dempster-Shafer, tem-se um teste de hipótese. No caso da abordagem empregada neste trabalho, as hipóteses deste teste são:

$H_0 : O\ organismo\ observado\ realizou\ atividades\ legítimas$
$H_a : O\ organismo\ observado\ realizou\ atividades\ potencialmente\ fraudulentas$

A estatística utilizada para discriminar a hipótese nula da hipótese alternativa foi o grau de anomalia S. Essa estatística S é calculada usando-se a teoria de Dempster-Shafer. No contexto de detecção de fraudes, o organismo de avaliação da conformidade pode ser classificado como fradulento F ou legítimo N, consequentemente, o quadro de discernimento para este contexto é $\Omega = \{F, N\}$. Por sua vez, o conjunto de hipóteses possíveis é $2^{\Omega} = \{\emptyset, F, N, U\}$, onde U representa o subconjunto$\{nem\ F\ nem\ N\}$. Para se obter o grau de anomalia de um determinado organismo de avaliação da conformidade, faz-se necessário modelar a função de probabilidade básica para todas as evidências que possam indicar a anormalidade desse organismo. Portanto, o grau de anomalia S de um organismo é o grau de crença associado a hipótese de anormalidade $Bel(F)$.

A técnica proposta inicia-se com o cálculo do grau de anomalia S para o organismo de avaliação da conformidade selecionado. Em seguida, amostram-se com reposição m objetos do conjunto de dados de todo o estudo para se formar pseudo-organismos, onde m é o número de objetos que compõem o organismo selecionado. Então, calcula-se o grau de anomalia S para cada pseudo-organismo criado. Repete-se esse procedimento η vezes, onde η é definido de acordo com o nível de significância desejado. Logo após, conta-se na distribuição empírica de S os valores do grau de anomalia que foram maiores ou iguais ao grau de anomalia observado para o organismo selecionado. Se esse valor for maior que $\alpha \times \eta$, aceita-se a hipótese nula H_0 para o organismo selecionado. Caso contrário, a hipótese alternativa é mais plausível. Aplica-se esse teste em todos os organismos que se deseja avaliar, os organismos com a hipótese nula rejeitada são marcados como potencialmente fraudulentos. Esses organismos podem ser alvo de visitas surpresas ou podem ter seus serviços analisados para verificar a existência de possíveis fraudes.

4.2 Análise dos serviços de avaliação da conformidade

Geralmente, um organismo de avaliação da conformidade realiza milhares de serviços por ano. Deste modo, para verificar se essas organizações estão prestando serviços legítimos, é imprescindível o desenvolvimento de ferramentas que permitam a avaliação dessas organizações de forma mais eficiente. A seguir são discutidas algumas propostas de métodos para esse fim.

4.2.1 Detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade usando Redes Neurais - *Learning Vector Quantization*

Nesta seção, apresenta-se uma proposta de método que utiliza uma técnica de classificação chamada LVQ para detecção de possíveis casos de fraudes em serviços de avaliação da conformidade. Tem-se como objetivo identificar os organismos fraudulentos, de modo a auxiliar as autoridades governamentais no combate às fraudes nessas organizações.

De posse de exemplos de dados contendo informações sobre características de organismos legítimos e fraudulentos, realiza-se o treinamento da rede neural LVQ. Depois, utiliza-se o modelo criado para classificar novas instâncias.

4.2.2 Detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade usando Processo de Decisão de Markov

Uma outra proposta apresentada neste trabalho é um método detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade baseado no Processo de Decisão de Markov (Markov Decision Process - MDP) (SOUZA; CARMO; PIRMEZ, 2014). O Processo de Decisão de Markov é um problema de decisão sequencial para um ambiente completamente observável, estocástico, com um modelo de transição de Markov e recompensas aditivas. A investigação realizada por auditores para verificar se a prestação de um serviço atende ou não a uma norma encaixa-se num problema de MDP. Um auditor, representando o agente do MDP, analisa registros em uma auditoria de forma sequencial. A cada novo registro analisado, o auditor decide qual fará parte de seu conjunto de evidências de atendimento a uma norma. Geralmente, não há tempo para analisar todos os registros

produzidos por uma empresa, assim ele escolhe um subconjunto desses registros, onde cada registro possui uma probabilidade de ser escolhido.

Além disso, os registros coletados são ligados pelos seus atributos em comum, sendo que a escolha do próximo registro depende dos atributos do registro atual. Para aplicação de um MDP considerar-se-á que a escolha do próximo registro depende apenas do atributos do registro atual. Registros anteriores não terão influência na decisão do próximo registro a compor um caso de suspeita de fraude. Com isso se estabelece a propriedade de Markov necessária a aplicação de um MDP. O objetivo da aplicação de um MDP é utilizar seu poder de planejamento para selecionar um subconjunto de dados com maior grau de suspeita de fraude.

4.2.2.1 Definindo o conjunto de estados e ações

A solução de um MDP consiste em estabelecer uma política ótima levando em conta a tupla (S, A, T, R). Onde tem-se o conjunto de estados S, o conjunto de ações A, função de recompensa R e a função de probabilidades T.

O conjunto de estados S pode ser definido como sendo os serviços realizados pelo organismo de avaliação da conformidade. De outro lado, o conjunto de ações A pode ser definido pelos atributos de cada serviço prestado.

4.2.2.2 Definindo a função de recompensa

A função de recompensa denotada por R deve ser escolhida de modo a indicar quais são os serviços suspeitos. Para isto, pode-se utilizar modelos de distribuições estatísticas ou outra métrica que indique desvios de procedimento na realização dos

serviços de avaliação da conformidade.

4.2.2.3 Definindo a função transição de probabilidades

A função de transição T indica as probabilidades que o agente do MDP pode transitar entre os estados possíveis do sistema. Essa transições conectam serviços realizados com atributos em comum, para formarem um subconjunto que de acordo com a recompensa acumulada pode se classificado como suspeito.

4.2.2.4 Estabelecendo uma política ótima

Uma vez que a tupla (S, A, T, R) da MDP está definida, pode-se utilizar o algoritmo 1 para se encontrar uma política ótima (DAVID; ALAN, 2010). O algoritmo 1 é chamado de iteração de valor assíncrona, pois o cálculo da função $Q(s, a)$ para cada par estado-ação é realizado em qualquer ordem. Além disso, vale destacar que o critério de parada indica que a diferença absoluta entre a função de valor $V(s)$ e a função de valor ótima $V^*(s)$ é menor que ϵ para todo s. Por fim, o algoritmo retorna a função $Q^*(s, a)$ para que seja obtida uma política sub-ótima. Este tipo de política será utilizada posteriormente em experimentos abordados neste trabalho.

4.2.2.5 Explorando o ambiente com a política ótima

De posse da política ótima, o agente deve explorar o conjunto de dados para listar os elementos suspeitos de fraude. Neste ponto, deve-se definir os pontos inicial e final de cada episódio de exploração do ambiente.

Algoritmo. 1 Iteração de Valor Assíncrona$(S, A, R, T, \gamma, \epsilon)$. Algoritmo para encontrar uma política ótima de um MDP.

início
inicia $\pi(s)$ arbitrariamente
inicia $Q(s, a)$ arbitrariamente
inicia $V_k(s)$ com zeros
$k := 0$
    repita
    $k := k + 1$
    seleciona randomicamente estado s
    seleciona randomicamente ação a
    $Q(s, a) := \sum_{s\prime} T(s\prime \mid s, a)(R(s\prime \mid s, a) + \gamma \max_{a\prime} Q(s\prime, a\prime))$
    $V_{k-1}(s) := V_k(s)$
    $V_k(s) := \max_a Q(s, a)$
    até $\forall s \mid V_k(s) - V_{k-1}(s) \mid < \frac{\epsilon(1-\gamma)}{\gamma}$
    para cada estado s **faça**
        $\pi^*(s) := \arg\max_a Q^*(s, a)$
    retorna $\pi^*, Q^*(s, a)$
fim

4.2.2.6 Lista dos dados suspeitos de fraude

O agente, usando a política ótima obtida, visitará vários estados dentro do conjunto de dados considerado. A lista de elementos suspeitos de fraude são todos esses estados visitados.

4.2.3 Detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade usando técnicas de agrupamento e de detecção de "outliers"

Também neste trabalho, apresenta-se uma proposta de método para descobrir anomalias nos resultados fornecidos por um organismo de avaliação da conformidade (SOUZA; CARMO; PIRMEZ, 2016). A Figura 4.2 mostra o fluxograma desse procedimento.

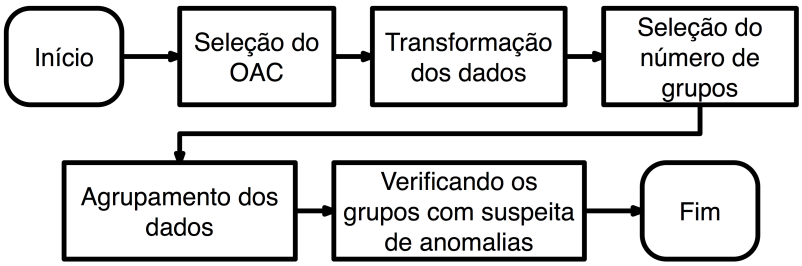


Figura 4.2: Fluxograma para o procedimento de análise dos resultados de um organismo de avaliação da conformidade

O primeiro passo é seleção do organismo a ser avaliado. Em seguida, realiza-se um pré-processamento dos dados para a consequente aplicação da técnica de agrupamento. Então, escolhe-se o número ótimo de grupos a serem analisados. Finalmente, identifica-se os grupos de dados mais suspeitos de conter anomalias. Estes grupos suspeitos serão bons candidatos para análises mais detalhadas.

4.2.3.1 Transformação dos dados

Algumas vezes, os dados selecionados necessitam de uma transformação antes da aplicação de uma técnica de agrupamento de forma que o trabalho seja realizado apropriadamente. Quando uma técnica de agrupamento é utilizada, todos os atri-

butos do conjunto de dados precisam ter o mesmo peso. A fim de se conseguir isso, usou-se o processo de normalização com z-score A Equação 4.1 mostra a fórmula para o cálculo do z-score onde $\bar{y}$ e σ representam a média e o desvio padrão do atributo y, respectivamente.

$$z = \frac{y - \bar{y}}{\sigma}. \tag{4.1}$$

4.2.3.2 Escolhendo o número de grupos

Técnicas de agrupamento separam objetos em grupos, onde os membros de um grupo são similares entre si, e são diferentes de outros objetos em outros grupos (WITTEN; EIBE; HALL, 2011). Geralmente, antes da aplicação das técnicas de agrupamento, não se tem conhecimento do número de grupos existentes no conjunto de dados. Para se superar esse problema, pode-se utilizar uma estratégia simples: iniciar de um determinado valor mínimo de grupos e avaliar outros valores até um determinado máximo, escolhendo então o número de grupos que se obteve o melhor resultado de acordo com um determinado indicador. Uma estimativa promissora é procurar esse número ótimo de grupos dentro do intervalo $[2, ||\sqrt{M}||]$, onde M é o número de objetos em um determinado conjunto de dados (PAL; JAMES, 1995), (HE; TAN, 2012).

Para avaliar qual seria o melhor número de grupos a ser usado na técnica de agrupamento, utilizou-se o índice de Calinski-Harabasz. Este indicador está positivamente associado ao grau de diferença entre grupos e negativamente associado à distância entre objetos dentro de um mesmo grupo (HE; TAN, 2012). As equações 4.2-4.4 mostram como o índice de Calinski-Harabasz é calculado:

$$V(K) = \frac{(M-K)B}{(K-1)W} \tag{4.2}$$

onde,

$$B = \sum_{i=1}^{K} |C_i|(w_i - w)^\top (w_i - w) \tag{4.3}$$

e,

$$W = \sum_{i=1}^{K} \sum_{x \in C_i} (x - w_i)^\top (x - w_i) \tag{4.4}$$

com V representando o índice de Calinski-Harabasz, $|C_i|$ como o número de objetos dentro de um grupo C_i, w como a média dos valores do conjunto de dados inteiro, w_i como a média dos objetos no grupo C_i, e K como o número de grupos.

Para se escolher o número de grupos, aplicou-se uma técnica de agrupamento para um determinado número de grupos K dentro do intervalo $[2, ||\sqrt{M}||]$. Depois, avaliou-se os grupos produzidos através do índice V até que todos os números de grupos dentro intervalo acima fossem avaliados. Finalmente, escolheu-se o número de grupos com o maior valor de V.

4.2.3.3 Agrupamento dos dados

De forma a melhorar a precisão de método de agrupamento em identificar grupos de resultados anômalos, no procedimento proposto, usa-se uma estrutura

em que se agrega aos atributos dos objetos os valores de anomalia associados a cada objeto integrante do conjunto de dados. As Equações 4.5 e 4.6 mostram as estruturas de agrupamento utilizadas neste estudo. A Equação 4.5 representa a estrutura original do conjunto de dados Rn considerando apenas os M resultados por N atributos do conjunto de dados do organismos de avaliação da conformidade. Por sua vez, a Equação 4.6 representa a estrutura agregada Ra, considerando M resultados por N atributos e M graus de anomalia por L técnicas para detecção de valores discrepantes, onde $L = 1, 2, 3 \cdots$ Essa estrutura agregada permite à técnica de agrupamento em estabelecer grupos onde elementos com grau de anomalia similares estejam juntos.

$$R\text{n} = \begin{bmatrix} Y_{1,1} & Y_{1,2} & \cdots & Y_{1,N} \\ Y_{2,1} & Y_{2,2} & \cdots & Y_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ Y_{M,1} & Y_{M,2} & \cdots & Y_{M,N} \end{bmatrix} \tag{4.5}$$

$$R\text{a} = \left[\begin{array}{cccc:ccc} Y_{1,1} & Y_{1,2} & \cdots & Y_{1,N} & A_{1,1} & \cdots & A_{1,L} \\ Y_{2,1} & Y_{2,2} & \cdots & Y_{2,N} & A_{2,1} & \cdots & A_{2,L} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ Y_{M,1} & Y_{M,2} & \cdots & Y_{M,N} & A_{M,1} & \cdots & A_{M,L} \end{array}\right] \tag{4.6}$$

Para calcular os graus de anomalia associado a cada objeto do conjunto de dados, usou-se técnicas de detecção de valores discrepantes. Esse grau de anomalia foi obtido de acordo com o tamanho do desvio entre a frequência esperada pela frequência observada no conjunto de valores com relação a uma distribuição estatística de referência. Quanto maior o desvio entre o valor observado para o valor esperado, maior é o grau de anomalia do objeto pertencente ao conjunto de dados sob estudo.

Para realizar o processo de agrupamento dos dados, utilizou-se uma técnica

popular chamada *k-means*, que toma pontos iniciais de forma aleatória no conjunto de dados para representar os centros dos grupos a serem formados. Todos os objetos são designados para o centro do grupo mais próximo, a média dos valores do grupo é calculada para forma o novo centro do grupo. (WITTEN; EIBE; HALL, 2011).

4.2.3.4 Verificando os grupos com suspeitas de anomalias

Nesse passo, procura-se identificar quais grupos são anômalos. Pode-se utilizar abordagens como a consideração de que, geralmente, dados legítimos pertencem a grupos grandes e densos, enquanto anomalias grupos pequenos e esparsos (CHANDOLA; BANERJEE; KUMAR, 2009). Também, pode-se levar em conta conhecimentos específicos do contexto da aplicação usando-se estatísticas descritivas, testes de hipótese, gráficos de probabilidade entre outras técnicas. Após se identificar os grupos de serviços anômalos, pode-se investigar com mais detalhes as evidências de realização desses serviços com intuito de verificar se houve alguma irregularidade. Nestes casos, pode-se analisar registros fotográficos ou filmagens dos serviços realizados.

4.3 Análise das filmagens dos serviços realizados

As filmagens dos serviços de avaliação da conformidade registram o passo a passo da execução desse serviço. Após realizar a seleção de serviços suspeitos de fraude usando os métodos apresentados anteriormente, o uso das filmagens dos serviços selecionados pode permitir a constatação objetiva do comportamento fraudulento. Nesta seção, apresenta-se uma proposta de método rápido para análise das filmagens dos serviços de um organismo de avaliação da conformidade.

4.3.1 Detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade usando filmagens de seus serviços

No método proposto, o primeiro passo é a seleção dos vídeos. Depois, estabelece-se o processamento dos vídeos selecionados. Em seguida, calcula-se o grau de anomalia para cada vídeo. Com esse grau de anomalia, um analista pode confirmar se existe um caso de fraude ou não dentro dos vídeos anômalos.

4.3.1.1 Seleção dos vídeos

A seleção dos vídeos pode ser uma saída das técnicas descritas em (SOUZA et al., 2013), (SOUZA; CARMO; PIRMEZ, 2014), (SOUZA; CARMO; PIRMEZ, 2016) ou um subconjunto de vídeos selecionados por uma amostragem aleatória dentro de um conjunto de serviços realizados pelo organismo de avaliação da conformidade.

Para seleção dos vídeos a serem analisados pelo método proposto, algumas considerações devem ser levadas em conta. A primeira delas é que a câmera esteja fixa e que o plano de fundo seja aproximadamente constante. Além disso, considera-se que as atividades monitoradas seguem um determinado protocolo e que essas atividades são realizadas conforme um disposição fixa no ambiente.

4.3.1.2 Processando os vídeos selecionados

Depois de selecionar uma conjunto de vídeos para serem analisados, o processamento dessas filmagens podem iniciar. Deve-se definir que informações podem indicar algum comportamento fraudulento, seja pela aparição de ações específicas,

objetos, cores e outros elementos que podem definir se um serviço foi realizado de forma legítima ou não.

Para tornar o processamento dos vídeos mais rápido, o procedimento proposto considera apenas os quadros estatisticamente diferentes. Para avaliar se um quadro é estatisticamente similar ou não com relação a outro quadro no vídeo, usa-se o histograma da escala de cinza dessas imagens. Uma representação na escala de cinza de uma imagem corresponde a uma matriz de pixels, usualmente de 8 bits por pixel, onde cada pixel de valor 0 corresponde a cor preta, e o pixel de valor 255 corresponde a cor branca, valores intermediários correspondem a tons de cinza. Por sua vez, o histograma de uma imagem é uma representação gráfica da frequência de ocorrência de cada nível de cinza na imagem (MARQUES, 2011). A ideia por trás da comparação baseada em histogramas é que quadros com pouca mudança no cenário ou na movimentação dos objetos têm pequena diferença em seus histogramas da escala de cinza (KOPRINSKA; CARRATO, 2001).

Para decidir se dois quadros consecutivos possuem histogramas similares, faz-se a normalização desses histogramas e depois usa-se o teste de Kolmogorov-Smirnov para duas amostras (SIEGEL, 1956). Como primeiro passo, um distribuição acumulada é feita para cada histograma normalizado na escala de cinza de dois quadro subsequentes. Para cada intervalo, uma distribuição acumulada é subtraída da outra. O valor LS da maior diferença entre essas duas distribuições é comparado com o valor crítico KS do teste Kolmogorov-Smirnov para duas amostras. A hipótese considerando a similaridade entre os dois histogramas normalizados na escala de cinza é rejeita, caso o valor LS seja maior que o valor KS obtido.

4.3.1.3 Determinando os vídeos anômalos

De posse da definição das informações que podem indicar sintomas de fraude nos serviços realizados pelo organismo de avaliação da conformidade, pode-se utilizar técnicas estatísticas para indicar quais vídeos contém serviços potencialmente fraudulentos. Neste ponto, pode-se analisar trajetórias mais comuns, frequência de aparição de um determinado objeto, ou outros elementos que possam indicar anomalias.

4.4 Investigação automática de casos similares

Depois de se comprovar um comportamento fraudulento após a análise da filmagem de um serviço de avaliação da conformidade, uma forma útil de se investigar automaticamente caso similares seria com a utilização de filmagens do serviços realizados. Nesta seção, apresenta-se uma proposta de um método para encontrar padrões incomuns em organismo de avaliação da conformidade usando retroalimentação. Deseja-se aproveitar o conhecimento de comportamentos fraudulentos detectados previamente, para se buscar automaticamente outros casos similares.

4.4.1 Extração de características das filmagens do serviços realizados

O primeiro passo consiste em extrair um conjunto de características dos vídeos que contém serviços prestados por um organismo de avaliação da conformidades. Para caracterizar a sequência de ações realizadas em cada vídeo durante o desempenho do serviço de avaliação da conformidade, pode-se usar o histograma orientado de fluxo ótico da cena em questão. Formalmente, pode-se definir a sequência de ações em um vídeo como sendo uma sequência de histogramas orientados de

fluxo ótico $S = h_1, h_2, ..., h_n$ onde h é o histograma orientado de fluxo ótico de uma determinada ação em uma cena e n é o número de ações registradas.

O histograma orientado de fluxo ótico é uma abordagem de representação global de uma cena. Diferentemente de uma abordagem local, essa técnica permite o entendimento da atividade observada como um todo. Sem contar que, ela permite estabelecer a evolução temporal de movimentos, o que se tornar interessante para se caracterizar a execução de um ensaio que deve seguir uma sequência predeterminada de passos. Além disso, o histograma orientado de fluxo ótico é invariante a escala e resistente a pequenas quantidades de ruído (CHAUDHRY et al., 2009).

4.4.2 Aplicação de técnicas de alinhamento de sequência

Inspirado na literatura de detecção de vírus metamórficos, pretende-se utilizar alinhamento de sequências para diferenciar instâncias legítimas de instâncias fraudulentas (MCGHEE, 2007). Um vírus metamórfico possui a capacidade de produzir cópias de si que são funcionalmente equivalentes e com estruturas internas diferentes (WONG; STAMP, 2006). Esse tipo de vírus pode utilizar várias estratégias em suas replicações, destacam-se: a inserção ou remoção de instruções desnecessárias; a substituição de instruções; e a transposição de trechos de códigos (SHANMUGAM; LOW; STAMP, 2013). Todas essas estratégias tem como objetivo disfarçar um comportamento malicioso por parte desse vírus. Geralmente, as ações de um vírus metamórfico podem ser representadas por uma sequências de elementos de código, os quais tendem a conservar propriedades estatísticas.

Considerando uma atividade de avaliação da conformidade como uma sequência de ações definidas por um protocolo. Pode-se representar essas atividades através de elementos que caracterizem as ações tomadas durante do desempenho da avalia-

ção da conformidade. Assumindo que um organismo de avaliação da conformidade pode se comportar como um vírus metamórfico, ou seja, ele pode usar de estratégias como inserção de tarefas desnecessárias, substituição de tarefas ou transposição de atividades para disfarçar um comportamento malicioso, é razoável assumir que o uso de técnicas empregadas na deteção de vírus metamórficos possa ser utilizada no contexto da avaliação da conformidade, como é o caso das técnicas de alinhamento de sequências. O uso de técnicas de alinhamento de sequência, neste caso, ganhou força, pois, diferente da aplicação de modelos ocultos de Markov como em (ATTALURI; MCGHEE; STAMP, 2009) e (WONG; STAMP, 2006), elas não exigem uma fase de treinamento, podendo ser então aplicadas diretamente para comparar instâncias legítimas e fraudulentas. Visto que se tem poucos dados para validação dos métodos elaborados nesta tese.

Tendo em vista que as atividades de avaliação da conformidade podem ter durações distintas, que muitas vezes, depende do conhecimento, habilidade e experiência do ator de tais atividades, deve-se então utilizar a técnica de alinhamento local Smith-Waterman (SMITH; WATERMAN, 1981). Uma vez que, as técnicas de alinhamento global pressupõem sequências de tamanhos similares.

Diante de duas sequências de histogramas orientados de fluxo ótico, realiza-se um processo de alinhamento local dos elementos dessas sequências. Para decretar se há correspondência entre os elementos de duas sequências, usa-se a distância Euclidiana entre eles. Caso essa distância seja menor que um limiar previamente definido, determina-se uma correspondência, casso contrário, tem-se uma não correspondência entre elementos. Se o usuário dispõe de sequências que representam serviços fraudulentos, essas sequências podem ser utilizadas como referências para avaliar outros serviços. Quanto maior o grau de similaridade das novas sequências em comparação com as referências mais suspeitas as novas sequências avaliadas serão.

4.5 Resumo

Este capítulo apresentou um arcabouço para detecção de possíveis serviços fraudulentos em organismos de avaliação da conformidade. Os módulos e técnicas que compreendem esse arcabouço foram detalhados. No próximo capítulo, serão apresentados os casos de validação desse arcabouço.

5 VALIDAÇÃO DOS MÉTODOS PROPOSTOS

Neste capítulo, apresentam-se os estudos de caso utilizados para validar as técnicas que compõe o arcabouço proposto. Como mencionado anteriormente, existem diversos tipos de ferramentas de avaliação da conformidade, a saber: ensaio, inspeção, certificação e acreditação. Porém, para validação do arcabouço proposto, foram utilizados casos na área de inspeção. Este foco se deve ao acesso de algumas informações e casos reais de fraude na avaliação da conformidade no âmbito da ferramenta de inspeção.

5.1 Estudo de caso 1

Neste estudo de caso, avalia-se a eficácia da da aplicação do método de Bootstrap com Dempster-Shafer para detecção de organismos de avaliação da conformidade com possíveis serviços fraudulentos.

5.1.1 Teste de desvio lateral para inspeção de segurança veicular

A inspeção de segurança veicular é um processo de avaliação de um veículo, visando verificar suas condições de segurança, para que seja permitida, ou não, sua circulação em vias públicas. Tal avaliação deve ser realizada em estações de inspeção, com o veículo apresentando-se em condições de limpeza, que possibilitem a observação da estrutura, sistemas, componentes e identificação (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 1998).

Um dos testes realizados para se avaliar a segurança de veículos é o teste de desvio lateral. O objetivo desse teste é verificar o paralelismo das rodas nos eixos do veículo. O ensaio é realizado usando a placa de desvio lateral. Este equipamento tem uma placa que se desloca transversalmente à direção de movimentação do veículo. Uma das rodas passa pela placa de teste, enquanto a outra permanece no solo. A placa se move de acordo com o movimento lateral das rodas. Esse movimento da placa de teste gera um sinal elétrico que é então processado. No fim, o equipamento mostra o valor do deslocamento lateral, em metros, por distância longitudinal em kilômetros (POZUELO; DÍAZ; BOADA, 2014). Sabe-se que o desvio lateral tem grande influência na dirigibilidade do veículo, bem como no consumo de combustível e desgaste dos pneus (QIAO; XU, 2010).

5.1.2 Reclamações sobre casos de fraude em inspeção de segurança veicular

Embora os veículos que passam por organismos de inspeção acreditados sejam submetidos a equipamentos automatizados de testes, existem indícios de que os mesmo são aprovados de forma irregular. Esse tipo de ocorrência aumenta os riscos de acidentes e de danos ao meio ambiente.

Alguns cidadãos encaminham para a CGCRE reclamações sobre fraudes que são cometidas em organismos acreditados. Exemplos de reclamações sobre comportamento fraudulento em organismos de inspeção acreditados na área de segurança veicular são:

Reclamação 1: " *O organismo de inspeção realiza a troca de um veículo em condições ruins por outro em boas condições a fim de mascarar resultados.*".

Reclamação 2: "*O organismo possui um programa de computador que permite fa-*

zer a edição dos resultados nos relatórios de equipamentos automatizados.".

Reclamação 3: "*O organismo de inspeção adultera o equipamento usado nos ensaios para emitir resultados falsos.*".

Quando a CGCRE recebe uma reclamação sobre casos de fraude, geralmente ela realiza uma visita surpresa ao organismo de inspeção para verificar o cumprimento de regulamentos técnicos e também apurar a procedência da reclamação.

5.1.3 Conjunto de Dados

O conjunto de dados utilizado nesse primeiro estudo de caso compreende medições reais de teste de desvio lateral fornecidos por seis organismos de inspeção acreditados na área de segurança veicular. Dois dos organismos que forneceram dados foram detectados em operações de fiscalização como tendo comportamento fraudulento. As fraudes ocorreram na adulteração dos resultados do teste da placa de desvio lateral. A Tabela 5.1 mostra a descrição dos dados utilizados neste estudo. Tem-se, nessa tabela, o quantitativo de medições de desvio lateral por organismo, e se o organismo foi detectado como fraudulento em operações de fiscalização. Todos os dados foram coletados no ano de 2014.

Tabela 5.1: Descrição do conjunto de dados com medições de desvio lateral e com a indicação se o organismos foi detectado como fraudulento

Organismo	Medidas	Fraudulento?
1	137	Não
2	142	Não
3	237	Sim
4	117	Não
5	130	Não
6	174	Sim

5.1.4 Modelando as funções de probabilidade básica

Para se utilizar a teoria de Dempster-Shafer com o método de Bootstrap, faz-se necessário modelar as funções de probabilidade básica para o conjunto de evidências disponíveis. O primeiro passo é identificar quais evidências podem ajudar na identificação de comportamentos fraudulentos em organismos de inspeção acreditados. Alguns padrões que podem revelar comportamentos fraudulentos são: preferência por dígitos, números arredondados, muitos valores discrepantes ou ausência de valores discrepantes, baixíssima variabilidade nos dados ou variabilidade exarcebada, picos estranhos ou dados muito assimétricos (BUYSE et al., 1999).

No caso de inspeção de segurança veicular, espera-se uma alta variabilidade nos resultados dos ensaios nos veículos. Existem vários fatores que podem contribuir para essa alta variabilidade de resultados. Por exemplo: quanto mais idade tem um veículo e quanto mais quilômetros rodados ele tem, maior é a chance de existirem falhas em seus componentes. Além disso, o modelo do veículo e o grau de manutenção dado por seus proprietários também podem aumentar o índice de falhas nos testes de segurança. Desta forma, o fraudador, muitas vezes, deve falsificar resultados para atingir os valores limites em que um veículo pode ser considerado seguro. E em consequência desse processo de falsificação de resultados, pode-se afetar a variabilidade dos dados obtidos por essa organização. Assim, a primeira evidência a ser analisada em busca de comportamentos fraudulentos é a variabilidade dos resultados de um organismo de inspeção em segurança veicular. Quanto mais baixa for a variabilidade dos resultados, mais suspeitos esses resultados serão.

Conforme mostrado antes nos exemplos de reclamações sobre casos de fraude em organismos acreditados, existem indícios de que algumas empresas estejam utilizando programas de computador para falsificar resultados de inspeção. Baseado no fato que os seres humanos não são bons em criar números aleatórios, outra forma

de se investigar a existência de comportamento fraudulento é a preferência por determinados dígitos (BUYSE et al., 1999). Assim, a segunda evidência ser utilizada no método proposto é a preferência por dígitos, isto é, a tendência de se usar alguns dígitos em detrimento de outros quando da falsificação de resultados. Quanto maior a preferência por determinados dígitos, maior é a suspeita de falsificação. Enfim, é importante destacar que outros eventos podem causar preferências por dígitos, por exemplo, equipamentos defeituosos.

Usando a variabilidade e a preferência por dígitos como evidências, pode-se modelar as funções básicas de probabilidade que compõe a teoria de Demspter-Shafer. Os valores retornados por essas funções podem ser interpretados como o grau de anomalia que essas evidência revelam sobre os dados em estudo.

5.1.4.1 Evidência 1 - Variabilidade

Para se medir a variabilidade dos resultados de um organismo de inspeção usou-se o desvio padrão desses dados. Para simplificar o modelo, usou-se uma função linear para representar a função de probabilidade básica correspondente a essa primeira evidência. Esta função mapeia os valores de desvio padrão σ no intervalo de [0, 1]. Para completar esse modelo, resta determina o domínio dessa função. Sabe-se que onde existam pelo menos três números em conjunto de dados, o desvio padrão nunca irá exceder 60 % da amplitude do intervalo (CROUCHER, 2004). No caso do teste de desvio lateral, a amplitude dos resultados desse teste é definida pelo intervalo de -15 m/km a 15 m/km (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 1998). Assim, para as medidas da placa de desvio lateral, tem-se uma amplitude de intervalo de 30, calculando-se 60 % de 30, obtém-se 18. Portanto, uma boa estimativa para o domínio do desvio padrão é $\sigma_{dom} = [0, 18]$.

A Equação 5.1 define a função de probabilidade básica para medir o grau de anomalia atribuído pelo desvio padrão das medidas obtidas no teste de desvio lateral em veículos.

$$\left.\begin{array}{l} m_1(F) = \Psi_1 \\ m_1(N) = 0 \\ m_1(U) = 1 - m_1(A) \end{array}\right\} \tag{5.1}$$

onde

$$\Psi_1(\sigma) = \frac{-\sigma}{18} + 1 \tag{5.2}$$

5.1.4.2 Evidência 2 - Preferência por dígitos

Para investigar se existe preferência por determinados dígitos dentro de um conjunto de dados, pode-se utilizar histogramas sobre a frequência de aparição do dígitos mais significativos dos números que compreendem esse conjunto. Neste estudo utiliza-se a frequência de aparição do primeiro dígito mais significativo das medições realizadas pelo organismo de inspeção.

De modo a comparar a distribuição de frequência do primeiro dígito das medidas de um organismo de inspeção com relação à distribuição dos demais organismos sob estudo, utiliza-se uma abordagem similar ao que foi empregada em (TAYLOR; MCENTEGART; STILLMAN, 2002). Essa abordagem consiste em se verificar a distância euclidiana da distribuição de frequência do primeiro dígito mais significativo para as medições de um organismo com relação a distribuição de frequência do primeiro dígito mais significativo das medições de todos os demais organismos

juntos. O primeiro passo nessa abordagem é calcular as proporções de frequência de cada primeiro dígito mais significativo das medições realizadas pelo organismo de inspeção. Este cálculo usa a razão entre a frequência do primeiro dígito mais significativo e a quantidade de medições do organismo de interesse. O resultado é um vetor com 10 valores de proporção de frequência referentes aos dígitos de 0 a 9, no caso $p_0, p_1, p_2, \ldots, p_9$. Em seguida, utiliza-se processo análogo para o cálculo da distribuição de frequência do primeiro dígito mais significativo para as medições de todos os demais organismos juntos, tomando-se a razão entre a frequência do primeiro dígito mais significativo e a quantidade de medições de todos os organismos restantes. Também se obtém um vetor com 10 valores de proporção de frequência correspondentes aos dígitos de 0 a 9, no caso $P_0, P_1, P_2, \ldots, P_9$.

Finalmente, usando esse dois vetores e a Equação 5.3 , pode-se calcular a distância d_{DP} entre as proporções do organismo de interesse com relação ao demais organismos sob estudo.

$$d_{DP} = \sqrt{(p_0 - P_0)^2 + \cdots + (p_9 - P_9)^2} \tag{5.3}$$

De posse de um indicador para comparar a preferência por dígitos entre organismos de inspeção, pode-se agora modelar a função de probabilidade básica para aplicação da teoria de Dempster-Shafer. Como nosso indicador mede a distância entre as proporções do organismo de interesse com relação ao demais organismos sob estudo, tem-se que quanto mais distante a distribuição de organismo estiver, maior é o grau de suspeita desse organismo com relação aos seus resultados.

Para simplificar o modelo, usou-se uma função linear para representar a função de probabilidade básica correspondente a essa segunda evidência. Esta função mapeia os valores da distância d_{DP} no intervalo de [0, 1]. Para completar esse

modelo, resta determinar o domínio dessa função.

Em uma situação extrema, um organismo de interesse pode revelar uma preferência apenas por um tipo de dígito mais significativo, enquanto a frequência de aparição do demais dígitos seria zero, por exemplo, $v_1 = (1, 0, 0, \ldots, 0)$. De outro lado, os organismos restantes poderiam demonstrar preferência por um dígito mais significativo diferente do que foi escolhido pelo organismo de interesse. Enquanto os outros dígitos teriam frequência de aparição zero para o restante das organizações, por exemplo, $v_2 = (0, 1, 0, \ldots, 0)$. Esta situação extrema leva a uma distância de $d_{DP} = \sqrt{(1-0)^2 + (0-1)^2 + \cdots + (0-0)^2} = \sqrt{2}$. Desta forma, uma boa estimativa para o domínio de d_{DP} é $d_{DPdom} = [0, \sqrt{2}]$

$$\left.\begin{array}{l} m_2(F) = \Psi_2 \\ m_2(N) = 0 \\ m_2(U) = 1 - m_2(A) \end{array}\right\} \tag{5.4}$$

onde

$$\Psi_2(d) = \frac{d}{\sqrt{2}} \tag{5.5}$$

A Equação 5.4 define a função de probabilidade básica para medir o grau de anomalia atribuído pela distância de preferência por dígitos.

Em cada modelo de função de probabilidade básica anterior, considerou-se, da mesma foram que em (DONG; SHATZ; XU, 2009) e de modo a simplificar o problema, que a função de probabilidade básica para $m(N)$ retorna sempre o valor zero.

5.1.5 Regra de Dempster para combinação de evidências

Para se combinar duas evidências independentes, pode-se utilizar as seguintes equações

$$Bel(F) = \frac{m_1(F)m_2(F) + m_1(F)m_2(U) + m_1(U)m_2(F)}{K} \tag{5.6}$$

$$Bel(N) = \frac{m_1(N)m_2(N) + m_1(N)m_2(U) + m_1(U)m_2(N)}{K} \tag{5.7}$$

$$Bel(U) = \frac{m_1(U)m_2(U)}{K} \tag{5.8}$$

onde

$$\begin{aligned} K = {} & m_1(F)m_2(F) + m_1(F)m_2(U) + m_1(U)m_2(F) \\ & + m_1(N)m_2(N) + m_1(N)m_2(U) \\ & + m_1(U)m_2(N) + m_1(U)m_2(U). \end{aligned} \tag{5.9}$$

tendo o quadro de discernimento é $\{F, N\}$ e o conjunto de hipóteses possíveis é $2^{\Omega} = \{\emptyset, F, N, U\}$, com $U = \{nem\ F\ nem\ N\}$.

Finalmente, para se combinar múltiplas evidências, pode-se calcular, por exemplo, $Bel(F)$ combinando-se qualquer par de evidências, depois combinando o resultado obtido com a terceira evidência, e depois combina-se esse novo resultado obtido com a quarta evidência e assim por diante (DONG; SHATZ; XU, 2009).

Para ilustrar o cálculo do grau de anomalia de um determinado organismo de inspeção no ensaio de desvio lateral, suponha que esse organismo possua desvio padrão $\sigma = 3$ e a distância de preferência por dígitos $d_{DP} = 1$. Deseja-se saber o grau de crença desse organismo de inspeção ser fraudulento $Bel(F) = S$. Tendo em vista que esse organismo pode ser legítimo N ou fraudulento F, tem-se um conjunto de discernimento de $\Omega = \{N, F\}$, consequentemente tem-se $2^{\Omega} = \{\emptyset, N, F, U\}$, onde $U = \{nem\ N\ nem\ F\}$. Por definição, $m(\emptyset) = 0$, desta forma, resta saber qual é o peso dado pelas evidências a cada possível estado do sistema para que se possa utilizar a regra de combinação de evidências referida acima e determinar $Bel(F)$.

Da Equação 5.1 e tomando-se $\sigma = 3$, tem-se:

$$\left.\begin{array}{l} m_1(F) = \frac{-3}{18} + 1 = 0,83 \\ m_1(N) = 0 \\ m_1(U) = 1 - 0,83 = 0,17 \end{array}\right\} \tag{5.10}$$

Da Equação 5.4 e tomando-se $d_{DP} = 1$, tem-se:

$$\left.\begin{array}{l} m_2(F) = \frac{1}{\sqrt{2}} = 0,69 \\ m_2(N) = 0 \\ m_2(U) = 1 - 0,69 = 0,31 \end{array}\right\} \tag{5.11}$$

Logo, usando-se as equações 5.6 e 5.9, obtém-se o grau de anomalia $Bel(F) = 0,94$.

5.1.6 Resultados

Nesta seção, apresentam-se os resultados do estudo de caso 1. Os experimentos foram implementados no MATLAB®. Escolheu-se um nível de significância $\alpha = 1$ %, o que leva a um número de iterações $\eta = 5000$. O valor de $\alpha = 1$ % foi escolhido, pois fornece forte evidência de que a hipótese nula não é verdadeira, caso o teste chegue a essa conclusão. A semente de geração de números aleatórios utilizada foi o número 15, escolhido de forma arbitrária.

A Tabela 5.2 mostra o intervalo de valores para o desvio padrão e para a distância de preferência de dígitos após $\eta = 5000$ rearranjos dos dados dos organismos de inspeção acreditados. Pode-se notar, que os valores gerados encontram-se dentro do domínio definido para as funções de probabilidade básica modeladas anteriormente.

Tabela 5.2: Intervalo de valores para o desvio padrão e para a distância de preferência de dígitos após $\eta = 5000$ reamostragens

Organismo	$\sigma_{intervalo}$	$DP_{intervalo}$
1	[2,07, 3,33]	[0,0173, 0,1815]
2	[2,17, 3,28]	[0,0173, 0,1876]
3	[1,91, 3,12]	[0,0130, 0,1272]
4	[2,05, 3,33]	[0,0159, 0,2136]
5	[2,06, 3,28]	[0,0178, 0,2633]
6	[2,06, 3,19]	[0,0189, 0,3746]

A Figura 5.1 mostra a distribuição estatística acumulada obtida empiricamente para cada organismos de inspeção acreditado sob estudo após $\eta = 5000$ reamostragens dos dados. Uma distribuição estatística acumulada retorna a probabilidade dos valores em um conjunto serem menores ou iguais a um determinado valor no conjunto de dados (DOWNEY, 2014). Nessa figura, também se pode notar a marcação do valor da estatística S para o organismo de inspeção estudado.

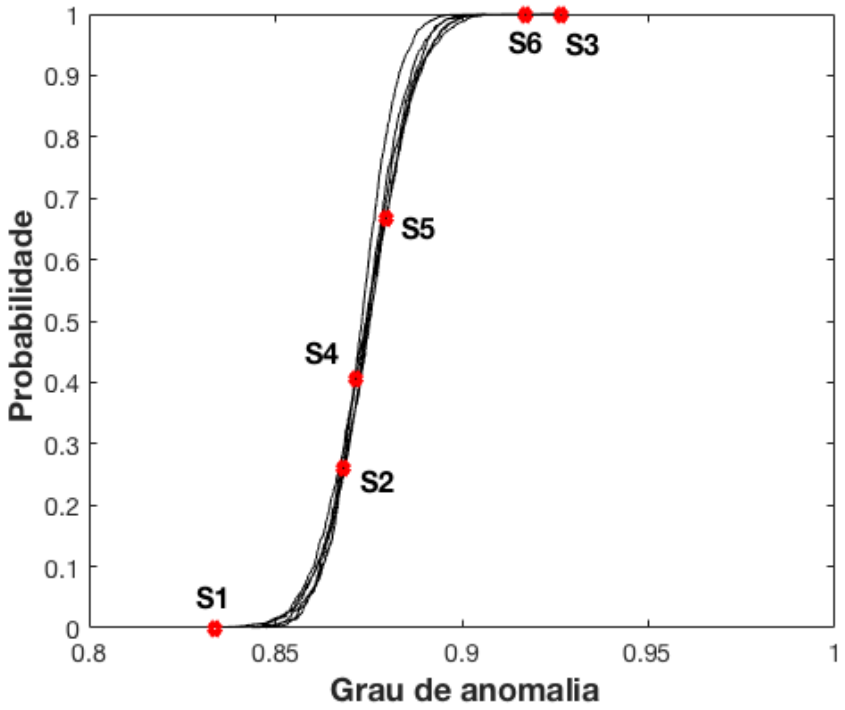


Figura 5.1: Distribuição estatística acumulada obtida empiricamente para cada organismos de inspeção acreditado sob estudo após $\eta = 5000$ reamostragens dos dados, onde S1, S2, S3, S4, S5 and S6 são os valores de grau de anomalia observados para os organismos 1, 2, 3, 4, 5 and 6, respectivamente.

Para o organismo 1, o valor do grau de anomalia é $S_1 = 0{,}8335$. Pode-se notar que a porcentagem de valores maiores ou iguais a S_1 é maior que o nível de significância escolhido, $\alpha = 1$ %. Precisamente, neste caso, o valor p é 100 %. Desta forma, aceita-se a hipótese nula para o organismo 1. Logo, não há evidência de que o organismo 1 seja anômalo. Em seguida, para o organismo 2, o valor do grau de anomalia é $S_2 = 0{,}8683$. Pode-se notar que a porcentagem de valores maiores ou iguais a S_2 é maior que o nível de significância escolhido, $\alpha = 1$ %. Precisamente, neste caso, o valor p é 75,72 %. Desta forma, aceita-se a hipótese nula para o organismo 2. Consequentemente, não há evidência de que o organismo 2 seja anômalo. De outro lado, para o organismo 3, o valor do grau de anomalia

para o organismo 3 é $S_3 = 0{,}9264$. Pode-se notar que a porcentagem de valores maiores ou iguais a S_3 é menor que o nível de significância escolhido, $\alpha = 1$ %. Precisamente, neste caso, o valor p é 0,02 %. Desta forma, rejeita-se a hipótese nula para o organismo 3. Consequentemente, o organismo 3 é marcado como sendo anômalo. Ainda, para o organismo 4, o valor do grau de anomalia é $S_4 = 0{,}8714$. Pode-se notar que a porcentagem de valores maiores ou iguais a S_4 é maior que o nível de significância escolhido, $\alpha = 1$ %. Precisamente, neste caso, o valor p é 60,48 %. Desta forma, aceita-se a hipótese nula para o organismo 4. Assim, não há evidência de que o organismo 4 seja anômalo. Seguindo, para o organismo 5, o valor do grau de anomalia é $S_5 = 0{,}8796$. Pode-se notar que a porcentagem de valores maiores ou iguais a S_5 é maior que o nível de significância escolhido, $\alpha = 1$ %. Precisamente, neste caso, o valor p é 30,88 %. Desta forma, aceita-se a hipótese nula para o organismo 5. Assim, não há evidência de que o organismo 5 seja anômalo. Por fim, para o organismo 6, o valor do grau de anomalia é $S_6 = 0{,}9170$. Pode-se notar que a porcentagem de valores maiores ou iguais a S_6 é menor que o nível de significância escolhido, $\alpha = 1$ %. Precisamente, neste caso, o valor p é 0,02 %. Desta forma, rejeita-se a hipótese nula para o organismo 6. Consequentemente, o organismo 6 é marcado como sendo anômalo.

O método proposto identificou com sucesso os organismos fraudulentos, visto que os organismos 3 e 6 receberam a decisão de se rejeitar a hipótese nula. Isto significa que os organismos 3 e 6 são anômalos em comparação aos demais participantes do estudo. Nota-se, que os graus de anomalia dos organismos são similares, no entanto, o valor p encontrado para os organismo 3 e 6 indicam que seus respectivos graus de anomalia raramente ocorreram em suas distribuições empíricas mostrando que esses organismos são de fato anômalos.

Por fim, vale destacar que um atacante poderia inserir dados com variabilidades artificiais, no entanto, esse tipo de ataque não foi considerado nesse estudo,

por ser um ataque mais complexo.

5.2 Estudo de caso 2

Neste estudo de caso, avalia-se a eficácia do uso de LVQ para detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade. Para esta avaliação, utilizou-se um cenário que envolve organismos de inspeção da área de transporte de produtos perigosos. O objetivo é realizar a classificação de organismos de inspeção legítimos e organismos de inspeção potencialmente fraudulentos.

5.2.1 Conjunto de dados

Devido à falta de um banco de dados com informações reais a respeito das inspeções na área de produtos perigosos, foi criado um banco de dados hipotético (SOUZA et al., 2013). Os atributos considerados nesse banco de dados foram retirados dos relatórios de supervisão dos organismos de inspeção. Os valores assumidos por esses atributos são valores típicos encontrados nas avaliações desses organismos.

Os atributos que compõem o banco de dados são: Número de Inspetores, Tempo da Inspeção Visual Interna, Tempo da Inspeção Visual Externa, Número de Bombas de Água, Vazão da Bomba de Água e Número de Inspeções por ano. A Tabela 5.3 mostra a faixa de variação para cada atributo do banco de dados.

Os valores dos atributos foram gerados usando a função ALEATORIOENTRE() do Excel. Esta função gera números aleatórios inteiros uniformemente distribuídos entre inteiros especificados. Isto tornou mais fácil a geração de valores para os atributos Número de Inspetores, Número de Bombas de Água e Número de

Tabela 5.3: Faixa de variação dos valores assumidos pelos atributos do banco de dados criado para este trabalho.

Atributos	Faixa de Variação
Número de Inspetores	2 a 6
Tempo da Inspeção Visual Interna (min)	10 a 60
Tempo da Inspeção Visual Externa (min)	10 a 60
Número de Bombas	1 a 3
Vazão das Bombas (m^3/h)	40 a 120
Número de Inspeções por ano	500 a 1800

Inspeções por ano que são típicos atributos de valores inteiros. Por simplificação também se usou a ALEATORIOENTRE() para gerar os valores dos atributos de Tempo da Inspeção Visual Externa e Tempo da Inspeção Visual Externa. Para o atributo vazão da bomba de água, usou-se a expressão ALEATORIOENTRE(1;6) x 20. Esta expressão gera aleatoriamente os valores 40, 60, 80, 100 e 120 m^3/h, que são valores típicos encontrados nos organismos de inspeção. O banco de dados foi construído de modo que todos os valores obtidos para os atributos do banco de dados ficassem dentro das faixas especificadas na Tabela 5.3.

O conjunto de dados possui um total de 500 amostras. A Figura 5.2 mostra uma parte desse conjunto dados criado com a indicação de seus atributos. Cada coluna representa um atributo diferente, e cada linha representa uma amostra.

5.2.2 Critério para indicação de fraude

Neste trabalho, criou-se uma a regra para caracterizar os organismos de inspeção como fraudulentos. Essa regra consiste em verificar se o número de inspeções declarado pelo organismo no conjunto de dados é maior do que o número de inspeções que ele pode realizar. O objetivo dessa regra é de simular casos sintéticos de fraude.

	A	B	C	D	E	F
1	Inspetores	TempInspVisInt	TempInspVisExt	Bombas	VazaoBomba	InspAno
2	6	54	24	1	120	1303
3	5	38	16	1	120	1443
4	6	47	48	2	120	854
5	6	23	58	1	100	1100
6	5	39	51	3	60	1143
7	3	51	46	2	40	1617
8	5	18	43	2	100	1717
9	2	54	24	1	80	1531
10	4	30	17	2	40	1441
11	4	44	17	1	120	1671
12	5	15	28	1	60	1671
13	3	52	15	1	80	1024
14	3	34	14	1	100	1289
15	2	31	38	1	120	1733
16	2	45	33	3	40	574
17	4	13	10	2	120	1593

Figura 5.2: Parte do conjunto de dados de inspeções produtos perigosos.

Para mensurar o número de inspeções que um organismo pode fazer, necessitou-se criar um modelo matemático baseado nos atributos do conjunto de dados. O modelo é estabelecido em um cenário idealizado. A Tabela 5.4 mostra as condições para determinação do número de inspeções que um organismo de inspeção pode fazer dadas as suas características operacionais. Os valores estabelecidos na Tabela 5.4 foram inspirados em valores típicos encontrados nas avaliações de organismos de inspeção na área de transporte de produtos perigosos. Assim, para se saber se um organismo é fraudulento nesse banco de dados criado, basta verificar se o número de inspeções declarado está acima do que ele pode fazer.

O número de inspeções que um organismo pode fazer de acordo com sua capacidade operacional é dado pela Equação 5.12.

Tabela 5.4: Regras do cenário idealizado para as inspeções em produtos perigosos.

Condições	Valores
Jornada de trabalho diária (h)	8
Volume do tanque inspecionado (L)	25000
Número inspetores por inspeção	2
Número de dias úteis por ano	260
As bombas de cada organismo possuem vazões iguais	-
Apenas uma bomba é utilizada por equipamento	-
Os organismos utilizam apenas o ensaio hidrostático	-
Recursos do organismo são ilimitados (ex: água abundante)	-
Demanda por inspeções constante o ano todo	-

$$Insp_{ano} = \begin{cases} \dfrac{260 \times 8}{tTinsp}\ ,\ se\ 2 \leq Inspt \leq 4 \\ \dfrac{260 \times 16}{tTinsp}\ ,\ se\ Inspt \geq 4\ e\ B = 2 \\ \dfrac{260 \times 24}{tTinsp}\ ,\ se\ Inspt = 6\ e\ B = 3 \end{cases} \tag{5.12}$$

sendo

$$tTinsp = \frac{tIint + tIext + tTmp}{60} + tTench + tTesv \tag{5.13}$$

e

$$tTench = tTesv = \frac{25}{VB} \tag{5.14}$$

onde,

Inspt número de inspetores;

B número de bombas de água;

tTinsp tempo total de uma inspeção (h);

tIint tempo da inspeção interna (min);

tIext tempo da inspeção externa (min);

tTench tempo de enchimento do tanque (h);

tTesv tempo de esvaziamento do tanque(h);

tTmp tempo de manutenção da pressão hidrostática (min);

VB vazão da bomba de água (m^3/h).

Os organismos de inspeção legítimos foram identificados através do valor 0, já os organismos fraudulentos foram identificados com o valor 1.

5.2.3 Resultados

A técnica de LVQ programa MATLAB®foi utilizada para gerar uma análise supervisionada do conjunto de dados. Essa análise leva em conta as classes dos dados, no caso organismos legítimos e organismos fraudulentos. Antes de aplicar a rede neural de LVQ no banco de dados deste trabalho, faz-se necessário realizar um pré-processamento dos dados. Este pré-processamento consiste na normalização dos dados. Essa etapa é necessária para que atributos de valores grandes não se sobreponham aos atributos com faixa de valores pequenos. Os dados de todos os atributos foram normalizados de modo que ficassem com média 0 e variância 1.

5.2.3.1 Classificação de organismos de inspeção em fraudulentos e legítimos

Nesta etapa, foram utilizados 500 exemplos sintéticos de características de organismos de inspeção. Sendo que 400 exemplos foram utilizados para treinamento da rede neural e 100 exemplos foram utilizados como conjunto de teste. Utilizou-se os parâmetros padrões do MATLAB B®para treinamento da rede, no caso, 10 camadas ocultas, taxa de aprendizado de 0,01, 50 épocas de treinamento, semente para gerar número aleatórios igual a 5, escolhido de forma arbitrária.

A Tabela 5.5 mostra os resultados da classificação feita pela rede elaborada neste trabalho. Dos 40 casos fraudulentos nas 100 amostras utilizadas para validação, a rede classificou corretamente 34 casos, errou 6 casos.

Tabela 5.5: Estatísticas das classificações de casos legítimos e fraudulentos.

Parâmetros	Valores
Total de amostras para validação	100
Total de casos legítimos no conjunto validação	60
Total de fraudes no conjunto validação	40
Acertos feitos pela rede para indicação de fraudes	35
Acertos feitos pela rede para indicação de casos legítimos	40
Indicações da rede com falso negativo	5
Indicações da rede com falso positivo	20

No entanto, houve 20 casos em que a rede indicou como fraudulentos, mas na realidade eles eram casos legítimos. Deste modo, das 55 indicações de fraude, o modelo da rede acertou 63,6 % das indicações de fraude.

Por sua vez, dos 60 casos de organismos de inspeção legítimos, a rede classificou corretamente 40 casos. Além disso, houve 5 casos fraudulentos que a rede indicou como casos legítimos. Sendo assim, das 45 indicações de casos legítimos, o modelo da rede acertou 88,8 % deles.

5.3 Estudo de caso 3

Neste estudo de caso, avalia-se a eficácia do uso do Processo de Decisão de Markov para detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade. Mais uma vez, são utilizados organismos de inspeção na área de segurança veicular. Especificamente, usa-se um conjunto de dados reais contendo medições realizadas em ensaios de emissão de poluentes veiculares. Usando esse conjunto de dados, simulou-se um ataque de clonagem de dados dentro dos resultados do organismo. Após esse ataque, aplicou-se o método proposto para se identificar quais serviços tinham sido adulterados.

5.3.1 Emissões veiculares e a Lei de Benford

Os requisitos para a realização das inspeções de segurança veicular estão dispostos nas Portarias Inmetro Nº 30/2004, Nº 32/2004 e Nº 49/2010. Uma das etapas dessa inspeção é a verificação do grau de emissão de monóxido de carbono (CO) e hidrocarboneto (HC) pelos veículos inspecionados. A emissão destes gases por automóveis segue uma distribuição estatística do tipo gama (HUI et al., 2007), (ZHANG; BISHOP; STEDMAN, 1994); e conforme os veículos vão envelhecendo e acumulando quilômetros rodados a tendência é que o grau de emissão aumente (WENZEL; BRETT; ROBERT, 2001). A intenção de se inspecionar os veículos quanto a emissão de poluentes é manter o índice de emissão dentro dos valores estabelecidos pelos órgãos ambientais.

Como mencionado anteriormente, algumas distribuições estatísticas como a exponencial, gama e log-normal atendem a Lei de Benford de forma aproximada (FORMANN, 2010). Portanto, espera-se que os resultados dos ensaios de emissões de gases poluentes encontrados pelos organismos acreditados sigam de forma

aproximada a Lei de Benford.

5.3.2 Definindo o conjunto de estados e ações para os ensaios de emissões veiculares

Primeiramente, usa-se uma representação tabular, onde cada linha da tabela representa um ensaio de emissão veicular realizado por um organismos de inspeção. Além disso, cada coluna representa um atributo desse ensaio. As linhas são o conjunto de estados possíveis S, onde cada linha é um estado s. Os atributos são o conjunto de ações A, sendo cada atributo uma ação.

A Tabela 5.6 ilustra como são representados os estados e ações. No exemplo mostrado nessa tabela, os dados contém informações sobre ensaios de emissões veiculares de gases poluentes. Os atributos são Vel velocidade de rotação do motor em marcha alta em rpm na hora do ensaio, $Fdil$ fator de diluição dos gases do ensaio, CO índice percentual de emissão de monóxido de carbono, $CO2$ índice percentual de emissão de dióxido de carbono e HC índice de emissão de Hidrocarboneto em ppm.

Tabela 5.6: Ilustração do conjunto de estados, ações e recompensas

Estados	Vel (rpm)	Fdil	CO(%)	CO2(%)	HC(ppm)	Recompensa
1	2571	1,67	0,13	8,83	42	0,84
2	2479	1,12	0,44	12,83	129	0,98
3	2547	1,00	0,01	13,51	16	1,19
4	2426	1,11	0,00	13,49	22	1,18

5.3.3 Definindo a função de recompensa usando a Lei de Benford

Para que se possa aplicar o Processo de Decisão de Markov, faz-se necessário definir a função de recompensa $R(s\prime \mid s, a)$. A recompensa de cada estado é associada com o grau de anomalia daquele estado. Neste estudo de caso, para definir esse grau de anomalia usou-se a Lei de Benford. A Tabela 5.6 ilustra a forma como as recompensas foram definidas. Para aplicação da Lei de Benford considerou-se apenas os dados de emissão de HC. Os valores de HC seguem uma distribuição estatística gama, logo espera-se que esses valores atendam a Lei de Benford de forma aproximada. Assim, o grau de anomalia de cada estado é determinado pelo grau de desvio que os valores de HC têm perante a Lei de Benford.

O grau de anomalia de cada estado s é calculado usando equação 5.15 descrita abaixo

$$Grau\ anomalia(s) = \frac{Prob_{observada}(s)}{Prob_{esperada}(s)} \tag{5.15}$$

onde $Prob_{observada}$ é a frequência observada dos dígitos mais significativos no conjunto de dados e $Prob_{esperada}$ é a frequência esperada dos dígitos mais significativos segundo a Lei de Benford (LU; BORITZ; COVVEY, 2006). A equação 5.16 define a função de recompensa do MDP

$$R(s\prime \mid s, a) = Grau\ anomalia(s\prime) = \frac{Prob_{observada}(s\prime)}{Prob_{esperada}(s\prime)} \tag{5.16}$$

Por exemplo, se forem usados os dois dígitos mais significativos dos elementos de um conjunto de dados e considerando o valor de HC no estado 1 da Tabela 5.6

, tem-se $D_1 = 4, D_2 = 2$. Suponha que essa combinação dos dois dígitos mais significativos apareça 12 vezes em um conjunto de dados de HC com 1400 elementos, então se teria $Prob_{observada} = 12/1400 = 0,0086$. A probabilidade esperada para os dois dígitos mais significativos quando $D_1 = 4, D_2 = 2$ é, segundo a equação 3.5, $Prob_{esperada} = 0,0102$. Portanto, o grau de anomalia/recompensa do estado 1 é 0,84.

5.3.4 Discretização dos dados

Com o intuito de se aplicar a técnica de Processo de Decisão de Markov, fez-se necessário discretizar os atributos do conjunto de dados. Quando os elementos do conjunto de dados não possuem classes atribuídas a eles, deve-se se lançar mão de técnicas de discretização não-supervisionadas.

Na literatura, existem duas técnicas bastante simples para discretização não-supervisionada, a primeira estabelece intervalos com larguras iguais e a segunda estabelece um número uniforme de elementos por intervalo. O número de intervalos N_{int} é escolhido *a priori* em ambas as técnicas (GARCIA; LUENGO; SAEZ, 2013). Neste trabalho, adotou-se a segunda técnica de discretização, pois a primeira pode retornar intervalos muito populosos e outros intervalos com poucos elementos, deixando o resultado da discretização enviesado. A Figura 5.7 mostra um exemplo de atributos discretizados, supondo um número de 200 intervalos. A coluna alvo não é mostrada, pois já foi utilizada para a determinação das recompensas.

5.3.5 Definindo a função transição de probabilidades T

Para se definir a função T, primeiro deve-se ter em mente que os estados são conectados através de atributos em comum. Considerando o método de discreti-

zação utilizado, onde o número de elementos N_e por intervalo é uniforme, apenas elementos de mesmo intervalo podem formar estados conectados. Admitindo transições equiprováveis, a probabilidade do agente sair de um estado s para um estado $s\prime$ escolhendo uma determinada ação a será $\frac{1}{N_e}$. Como o número de elementos de cada intervalo $N_e = N_s/N_{int}$, então a probabilidade de transição de um estado para o outro é $\frac{1}{N_e} = \frac{N_{int}}{N_s}$. Assim, a função de transição $T(s\prime \mid s, a)$ pode ser definida pela equação

$$T(s\prime \mid s, a) = \frac{N_{int}}{N_s} \tag{5.17}$$

onde N_s é o número total de estados.

Tabela 5.7: Atributos com valores discretizados

Estados	Vel (rpm)	Fdil	CO(%)	CO2(%)	Recompensa
5	110	1	166	91	1,41
6	126	173	158	31	1,22
7	9	1	167	94	0,49
8	135	1	160	41	1,11

Para exemplificar como as transições entre estados acontecem, considere que o agente só pode transitar entre os estados mostrados na Tabela 5.7. A figura 5.3 mostra o diagrama de transições da mudança de estados que o agente pode realizar nessa situação. Suponha que o agente está no estado 5 e escolhe a ação $Fdil$, o conteúdo de $Fdil$ no estado 5 é 1, logo os estados 7 e 8 estão conectados a 5. Uma vez escolhida a ação $Fdil$ no estado 5, e se verificando os estados conectados a esse estado, a decisão do próximo estado do agente será feita através de um sorteio. Cada próximo estado tem a mesma probabilidade de ser sorteado. Inclui-se nesse sorteio também o estado 5, já que ele próprio possui o conteúdo 1. Isso significa que o agente pode tomar uma ação e permanecer em seu estado atual. Assumindo transições equiprováveis, a probabilidade de transição entre os estados 5, 7 e 8 é

de 1/3. Caso no sorteio o agente saia do estado 5 e cai no estado 8, ele recebe a recompensa 1, 11. Isto é representado na figura 5.3 pela tupla (1; 0,333; 1,11), onde o primeiro elemento representa o valor da ação escolhida, o segundo representa a probabilidade da transição e o terceiro, a recompensa a ser recebida ao final da transição.

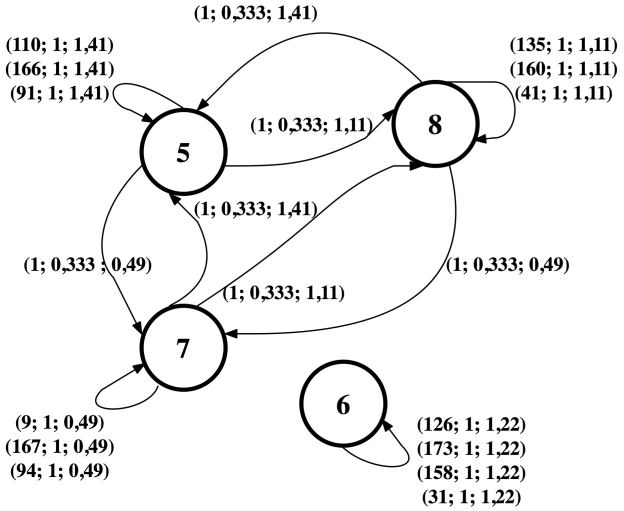


Figura 5.3: Representação gráfica do diagrama de transições.

5.3.6 Explorando o ambiente com a política ótima

De forma similar a (LU; BORITZ; COVVEY, 2006), a exploração ocorrerá em episódios. Um episódio é o trajeto do agente do estado inicial ao estado final. O estado inicial considerado neste trabalho é o estado cuja função de valor de estado é máxima, o estado final será qualquer estado previamente visitado.

5.3.7 Lista dos dados suspeitos de fraude

O agente, usando a política ótima obtida, visitará vários estados dentro do conjunto de dados considerada. A lista de elementos suspeitos de fraude são todos esses estados visitados.

5.3.8 Resultados

O desempenho do mecanismo proposto neste trabalho foi medido através de 4 experimentos. Esses experimentos foram elaborados usando programa MATLAB®. A semente de geração de números aleatórios utilizada foi o número 15, escolhido de forma arbitrária. Tais testes foram utilizados para verificar a capacidade do mecanismo em determinar um subconjunto de elementos onde se tenha o máximo grau de suspeita de fraude. Para isso, tomou-se um conjunto de dados de 1400 ensaios reais de emissão veicular de gases poluentes obtidos num organismo acreditado e tabulados numa planilha Excel®. Nesse conjunto de dados, simulou-se o ataque de um fraudador escolhendo aleatoriamente uma quantidade predeterminada de ensaios para serem adulterados. Nesses ensaios escolhidos aleatoriamente, foi alterada a medida de HC por um valor constante qualquer escolhido de forma arbitrária. No fim, aplicou-se o mecanismo proposto neste trabalho para verificar quantos elementos alterados eram detectados. A equação 5.18 mostra a métrica utilizada na medição do desempenho

$$TA_{med} = \frac{N_{alt}}{N_{rec}} \tag{5.18}$$

onde TA_{med} é a taxa média de acerto, N_{alt} é o número de elementos alterados e N_{rec} é o número de elementos recomendo pelo mecanismo proposto neste trabalho

como sendo anômalos. A média é calculada por episódio de exploração. A figura 5.4 mostra parte do conjunto de dados utilizados nos experimentos deste trabalho. Os atributos Vel, $Fdil$, CO, $CO2$ e HC são como explicados anteriormente.

F	G	H	I	J
Vel (rpm)	FDIL	CO (%)	CO2(%)	HC(ppm)
2589	1,09781033	0,0973125	13,56625	34,5625
2431	1,09901684	0,0754375	13,573125	40,9375
2574	1,11591575	0	13,441875	28,375
2414	1,12238694	0	13,364375	26,8125
2666	1,11198113	0,0500625	13,439375	55,6875
2475	1,10639867	0	13,5575	49,75
2571	1,67256711	0,13575	8,8325	42

Figura 5.4: Parte dos dados utilizados nos experimentos deste trabalho.

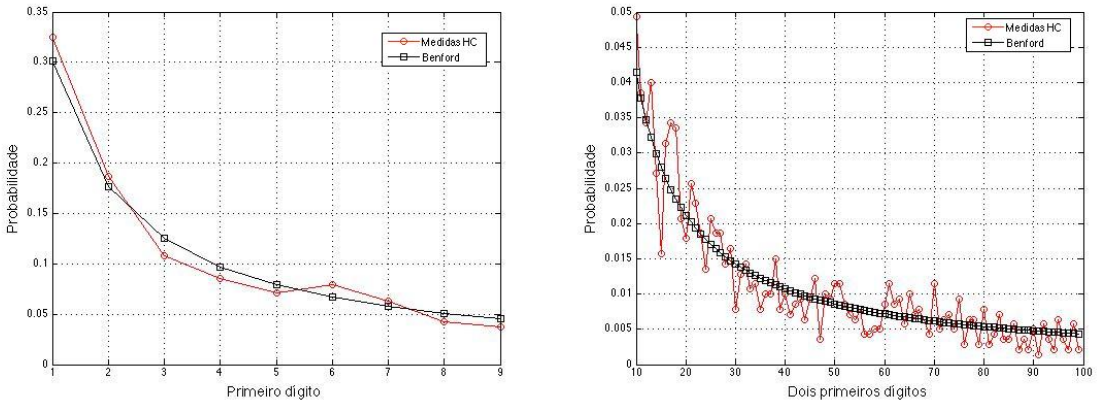
Considera-se $\gamma = 0,9$ como em (DAVID; ALAN, 2010); e uma precisão decimal de $\epsilon = 0,001$. Também considerou-se 121 episódios de exploração. Esse número de episódios de exploração foi escolhido para que se tivesse num número de graus de liberdade de 120. Com esse número de graus de liberdade, calculou-se os limites do intervalo de confiança da taxa média de acerto usando a distribuição estatística t e intervalo de confiança de 5%.

5.3.8.1 Influência da função de recompensa

Nesse primeiro experimento, o intuito é investigar de que forma a definição da função de recompensa pode influenciar na taxa média de acerto do mecanismo proposto neste trabalho. Duas opções foram utilizadas para definição da função de recompensa. A primeira opção considerou o grau de anomalia dado pela Lei de Benford usando apenas o primeiro dígito mais significativo. A segunda opção considerou os dois primeiros dígitos mais significativos.

As figuras 5.5 e 5.6 mostram os resultados obtidos a partir da aplicação da Lei de Benford ao conjunto de valores de HC. A figura 5.5 mostra a aplicação da Lei

de Benford considerando que os dados não sofreram nenhum tipo de adulteração. Já a figura 5.6 mostra a aplicação da Lei de Benford quando 140 valores de HC foram escolhidos aleatoriamente e adulterados para o valor de 17 ppm. O valor de 17 ppm foi escolhido de forma arbitrária, podendo ser outro valor de 2 dígitos. Nota-se na figura 5.6(a) que o dígito 1 apresenta o maior grau de anomalia. Na figura 5.6(b), o número 17 apresenta maior grau de anomalia. Ambas as figuras 5.6(a) e 5.6(b) indicam sinais de adulteração dos dados de HC.



(a) Lei de Benford com o primeiro dígito mais significativo

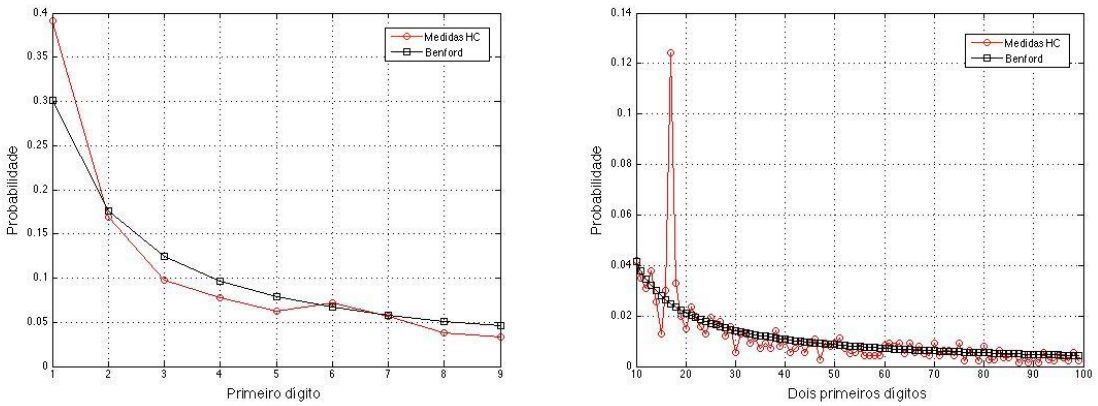
(b) Lei de Benford com os dois primeiros dígitos mais significativo

Figura 5.5: Aplicação da Lei de Benford no conjunto de valores de HC considerando o primeiro dígito mais significativo e os dois primeiros dígitos mais significativos sem adulterações.

Tabela 5.8: Desempenho considerando primeiro e segundo dígitos

Dígito mais significativo	Taxa média de acerto
Primeiro	$0,00 \pm 0,00$
Dois primeiros	$0,46 \pm 0,03$

Considerando o grupos de dados adulterados, aplica-se o MDP afim de se identificar quais elementos foram adulterados. Usou-se o processo de discretização de atributos com número de intervalos $N_{int} = 200$. A tabela 5.8 mostra os valores da taxa média de acerto.



(a) Lei de Benford com o primeiro dígito mais significativo

(b) Lei de Benford com os dois primeiros dígitos mais significativo

Figura 5.6: Aplicação da Lei de Benford considerando o primeiro dígito mais significativo e os dois primeiros dígitos mais significativos. No conjunto de valores de HC há 140 valores adulterados para 17 ppm.

Observa-se que usando os dois dígitos mais significativos pôde-se identificar mais elementos adulterados. O uso da Lei de Benford considerando os dois dígitos mais significativos permitiu focar as maiores recompensas nos valores que possuíam 1 e 7 como os dois primeiros dígitos mais significativos. Isso aumentou a chance de se encontrar mais elementos adulterados.

5.3.8.2 Influência do processo de discretização

Nesse segundo experimento, investiga-se a forma como a definição do número de intervalos pode influenciar na taxa média de acerto do mecanismo proposto neste trabalho. Para tal, tomou-se os seguintes números de intervalos $N_{int} = 100$, $N_{int} = 200$, $N_{int} = 280$ e $N_{int} = 350$. A função de recompensa foi definida pela Lei de Benford usando os dois primeiros dígitos mais significativos. Considera-se ainda que o número de elementos adulterados é de 140 valores, todos adulterados para o valor de 17 ppm de forma aleatória. A tabela 5.9 mostra os valores da taxa média de

acerto para cada valor de N_{int}.

Tabela 5.9: Desempenho considerando o número de intervalos

Intervalos	Taxa média de acerto
100	$0,23 \pm 0,03$
200	$0,46 \pm 0,03$
280	$0,67 \pm 0,04$
350	$0,18 \pm 0,03$

O número de intervalos tem influência direta na função de probabilidade das transições entre estados, bem como no número de estados que podem ser conectados entre si. Nota-se na tabela 5.9 que, aumentando o número de intervalos, tem-se um melhora na taxa média de acerto. No entanto, aumentar excessivamente o número de intervalos diminui a capacidade de acerto, já que diminui o número de estados que podem ser conectados entre si.

5.3.8.3 Influência da taxa de contaminação

Nesse terceiro experimento, verifica-se o efeito de se ter diferentes números de valores de HC adulterados. A função de recompensa foi definida pela Lei de Benford usando os dois primeiros dígitos mais significativos. Considera-se número de intervalos discretizados $N_{int} = 200$. Os valores de HC foram adulterados para o valor de 17 ppm de forma aleatória.

A tabela 5.10 mostra a taxa média de acerto quando o número de valores adulterados varia. Nota-se nessa tabela que quanto mais dados adulterados mais o mecanismo proposto neste trabalho consegue acertar. No entanto, é importante destacar que a Lei de Benford possui baixa sensibilidade. Quando poucos dados são modificados, a técnica não consegue destacar essas adulterações.

Tabela 5.10: Desempenho considerando número de elementos alterados

Número de alterações de HC	Taxa média de acerto
14	$0,00 \pm 0,00$
60	$0,00 \pm 0,00$
140	$0,46 \pm 0,03$
280	$0,47 \pm 0,04$
320	$0,69 \pm 0,04$

5.3.8.4 Influência da política utilizada

Por fim, neste quarto experimento, investiga-se a influência de se usar uma política ótima e outra sub-ótima para se listar os dados suspeitos de adulteração. A função de recompensa foi definida pela Lei de Benford usando os dois primeiros dígitos mais significativos. Considera-se número de intervalos discretizados $N_{int} = 200$. Os valores de HC foram adulterados para o valor de 17 ppm de forma aleatória. O número de valores adulterados foi de 140.

A tabela 5.11 mostra a taxa média de acerto quando se usa a política ótima e quando se usa a política sub-ótima. Como era de se esperar, usando a política ótima o agente consegue encontrar mais valores adulterados do que usando a política sub-ótima.

Tabela 5.11: Desempenho considerando política ótima e subótima

Política	Taxa média de acerto
Ótima	$0,46 \pm 0,03$
Sub-ótima	$0,11 \pm 0,02$

Por ilustração, a figura 5.7 mostra um episódio de exploração de um conjunto de dados e a lista de dados suspeitos de adulteração. Nesse exemplo, o mecanismo proposto neste trabalho recomenda quatro ensaios como adulterados, e consegue acertar os quatro.

```
Episódio( 20.000000 ).
( 182.00 ) - Vel(rpm) - 2441.00 Fdil - 1.17 CO - 0.36 - CO2 - 12.47 HC - 17.00
 ( 321.00 ) - Vel(rpm) - 2513.00 Fdil - 1.17 CO - 0.72 - CO2 - 12.11 HC - 17.00
 ( 770.00 ) - Vel(rpm) - 2374.00 Fdil - 1.17 CO - 0.00 - CO2 - 12.83 HC - 17.00
 ( 919.00 ) - Vel(rpm) - 2483.00 Fdil - 1.17 CO - 0.86 - CO2 - 11.97 HC - 17.00
```

Figura 5.7: Lista de ensaios suspeitos de fraude com política ótima, 4 recomendações e 4 acertos.

Já a figura 5.8 mostra um exemplo de episódio onde a lista de dados suspeitos de adulteração é dada pelo uso da política sub-ótima. Embora liste mais valores como sendo suspeitos, só um deles foi de fato adulterado.

```
Episódio( 120.000000 ).
( 1.00 ) - Vel(rpm) - 2589.00 Fdil - 1.10 CO - 0.10 - CO2 - 13.57 HC - 34.56
 ( 190.00 ) - Vel(rpm) - 2340.00 Fdil - 1.09 CO - 0.00 - CO2 - 13.79 HC - 18.50
 ( 208.00 ) - Vel(rpm) - 2463.00 Fdil - 1.10 CO - 0.00 - CO2 - 13.70 HC - 63.69
 ( 414.00 ) - Vel(rpm) - 2526.00 Fdil - 1.09 CO - 0.02 - CO2 - 13.68 HC - 14.75
 ( 663.00 ) - Vel(rpm) - 2534.00 Fdil - 1.10 CO - 0.13 - CO2 - 13.57 HC - 17.00
```

Figura 5.8: Lista de ensaios suspeitos de fraude com política sub-ótima, 5 recomendações e 1 acerto.

5.4 Estudo de caso 4

Nesse estudo de caso, avalia-se a eficácia da aplicação de técnicas de agrupamento e de detecção de "outliers" para detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade. Para validar essa proposição, também, utilizou-se um conjunto de dados reais de um organismo de inspeção em segurança veicular no que tange aos ensaios de emissões de poluentes veiculares. Usando esse conjunto de dados, simulou-se alguns ataques de fabricação de dados. Após os ataques, aplicou-se o método proposto para se identificar quais serviços tinham sido adulterados.

5.4.1 Parâmetros da distribuição estatística de emissões veiculares

As emissões veiculares são altamente variáveis. Essas emissões são afetadas por vários motivos: questões socioeconômicas, tecnologia do veículo, idade, kilômetros percorridos, modelo do veículo, grau de manutenção e mau uso do veículo (WENZEL; BRETT; ROBERT, 2001). Além disso, a distribuição estatística das emissões veiculares são altamente assimétricas e altamente leptocúrticas. Valores de assimetria e curtose observados na literatura para a distribuição estatística de emissões veiculares de CO em rodovias são : 1) (0,90, 2,28) e (1,21, 7,80) (HUI et al., 2007) ; 2) (2,60, 4,20) e (10,14, 26,46) (ZHANG; BISHOP; STEDMAN, 1994), respectivamente. Por sua vez, para emissções veiculares de HC em rodovias observou-se valores de assimetria e curtose iguais a: 1) (0,70, 13,54) e (0,77, 274,99) (HUI et al., 2007); e 2) (2,40, 17,00) e (8,64, 433,50) (ZHANG; BISHOP; STEDMAN, 1994), respectivamente. Nota-se que as distribuições de CO e HC tem valores positivos e altos para os parâmetros de assimetria e curtose. Esse conhecimento específico sobre as características das distribuições estatísticas de CO e HC serão base para seleção de grupos anômalos quando da aplicação do método proposto para a segunda fase do sistema de monitoramento de organismo de avaliação da conformidade. Basicamente, investiga-se os parâmetros de curtose e assimetria nos grupos formados pelo método proposto.

5.4.2 Conjunto de dados

O conjunto de dados de estudo de caso contém 526 medições reais de emissões de poluentes veiculares que foram fornecidas por um organismo de inspeção acreditado na área de segurança veicular. Todas as medições foram realizadas em 2014. A Tabela 5.12 os atributos que constituem esse conjunto de dados.

Tabela 5.12: Descrição dos atributos das medições de emissões de poluentes veiculres

Atributo	Descrição
Ano de fabricação	Ano em que o veículo foi fabricado
Quilômetros percorridos, km	Número de quilômetros viajados pelo veículo
ϕ(CO), %	Monóxido de Carbono contido na exaustão dos gases %
$\phi(CO_2)$, %	Dióxido de Carbono contido na exaustão dos gases %
ϕ(HC), 10^{-6}L/L	Concentração de Hidrocarboneto coletada pela sonda no escapamento do veículo
Fdil	Porcentagem volumétrica de diluição da amostra de gases de escapamento devida à entrada de ar no sistema, $F\text{dil} = 15 \ / \ (\phi(\text{CO}) + \phi(CO_2))$
ϕcorr(CO), %	Monóxido de carbono corrigido, $\phi\text{corr(CO)} = F\text{dil} \times \phi(\text{CO})$
ϕcorr(HC), 10^{-6}L/L	Concentração de Hidrocarboneto corrigida, $\phi\text{corr(HC)} = F\text{dil} \times \phi(\text{HC})$
Velocidade, RPM	Velocidade de rotação do motor com o veículo em ponto neutro

5.4.3 Modelos de ataque para adulteração de valores das medições de um organismo de avaliação da conformidade

Fraudadores possuem muitas técnicas para realizarem suas atividades fraudulentas em um organismo de inspeção. Por exemplo, os fraudadores podem clonar resultados, trocar objetos de inspeção, adulterar equipamentos de medição e editar resultados em certificados de inspeção. Neste estudo de caso, modelou-se as técnicas de clonagem de resultados e troca de resultados por outros valores gerados aleatoriamente em um intervalo predefinido.

5.4.3.1 Clonagem de resultados

Os fraudadores podem utilizar valores arbitrários para realizar suas atividades de clonagem de resultados. Ou de outro modo, eles podem ser mais cautelosos de modo a evitar chamar a atenção. Assim, dados falsificados tendem a não conter valores muito discrepantes, que possuem alto risco de serem detectados (BUYSE et al., 1999). Neste caso, simulou-se um fraudador que faz clonagem de resultados de acordo com a média das medições do conjunto de dados. Para isso, o primeiro passo consiste no cálculo da média dos valores do alvo a ser falsificado usando a equação:

$$\bar{X} = \frac{1}{n} \sum_{i=1}^{n} X_i \tag{5.19}$$

Depois, um subconjunto de valores é escolhido e essas medições são trocadas por esse valor médio $\bar{X}$ calculado anteriormente.

5.4.3.2 Substituindo resultados por valores aleatórios

Neste caso, escolhe-se no conjunto de dados um subconjunto de medições alvo, essas medições são substituídas por valores aleatórios gerados em um intervalo de X_1 to X_2. O tipo de distribuição a ser utilizada pelo gerador de número aleatório vai depender do fenômeno que se deseja simular, pode-se por exemplo, simular um atacante que tem uma ligeira preferência por determinado valor, ou pode-se usar uma distribuição uniforme, onde todos os valores tem a mesma chance se serem escolhidos.

5.4.4 Simulando o ataque de fraudadores

Neste estudo de caso, o organismo de inspeção é o ator que comete a fraude. Essa fraude ocorre quando a empresa emite um certificado de inspeção sem que o serviço tenha sido realizado, ou esse certificado contenha resultados falsificados. A principal motivação do fraudador é obter lucros e evitar conflitos com seus clientes devido a reprovação de seus veículos. Em organismo de inspeção em segurança veicular os fraudadores, geralmente, tem como alvo os veículos que possuem alta probabilidade de falhar em algum teste de segurança ou de emissões de poluentes.

No caso de ensaios de emissões de poluentes veiculares, em (BIN, 2003), consta que veículos com idade acima de 10 anos ou com 144000 km quilômetros percorridos possuem uma alta probabilidade de falharem no teste de emissões de poluentes. Por sua vez, em (MILOSAVLJEVIĆ; PEŠIĆ; DAŠIĆ, 2015), menciona que veículos com mais de 10 anos de idade possuem 41% de chance de falhar no teste de emissões, e que para modelos europeus e americanos, quando o número de quilômetros rodados ultrapassa a marca de 100000 km as chance de reprovação nesse teste também aumentam. Desta forma, para simplificar o cenário e conciliar essas duas fontes de informação, na simulação do ataque de um fraudador, no conjunto de dados sobre emissões veiculares, adulterou-se, propositalmente, os valores de emissões dos veículos com mais de 10 anos de idade ou com mais de 144000 km quilômetros percorridos. Cabe destacar que no conjunto de dados sob estudo, 95% dos veículos são modelos de montadoras européias ou americanas. A Figura 5.9 mostra distribuição das marcas de veículos dentro do conjunto de dados sob estudo

Por questões de simplificação, simulou-se o ataque de um fraudador apenas para os valores de emissões de HC. Esta simplificação se mostra razoável, uma vez que veículos com alto grau de emissão de CO também tendem a ter alto grau de emissão de HC (WENZEL; BRETT; ROBERT, 2001). Consequentemente, frauda-

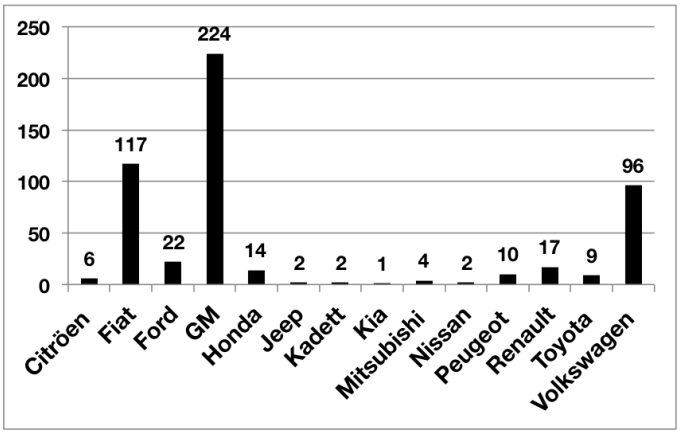


Figura 5.9: Distribuição das marcas de veículos dentro do conjunto de dados sob estudo.

dores que almejarem adulterar valores de CO, provavelmente terão de adulterar os valores de HC.

5.4.5 Calculando o grau de anomalia de cada objeto no conjunto de dados

Para calcular o grau de anomalia associado a cada objeto do conjunto de dados, usou-se duas distribuições estatísticas de referência: a Lei de Benford e a distribuição estatística Gama. Essa distribuições foram utilizadas como referência para verificar o grau de desvio das medidas de HC.

Na aplicação da Lei de Benford, considerou-se o primeiro e o segundo dígitos mais significativos para as medições de HC. O grau de anomalia para cada objeto do conjunto de dados foi determinado pelo desvio da frequência observada para o primeiro e segundo dígitos mais significativos com relação a frequência esperada pela Lei de Benford.

Na aplicação da distribuição estatística Gama, o grau de anomalia de cada objeto foi calculado através do desvio da frequência observada para uma determinada medição com relação ao valor esperado de acordo com essa distribuição estatística. Consequentemente, na estrutura agregada para realizar agrupamento pode-se ter mais três colunas representando os graus de anomalias mencionados.

5.4.6 Avaliação da eficácia do método proposto

Para avaliar o método proposto para análise de resultados de um organismo de avaliação da conformidade, adotou-se a porcentagem de resultados apontados como suspeitos que se concretizaram como sendo valores adulterados (θ) e a porcentagem de dados que foram identificados como adulterados dentro do conjunto de dados adulterados (ζ) (AGGARWAL, 2013). As Equações 5.20 e 5.21 mostram como calcular os valores de θ e ζ,

$$\theta = \frac{S \cap G}{S} \tag{5.20}$$

$$\zeta = \frac{S \cap G}{G} \tag{5.21}$$

onde o conjunto declarado como anômalo é denotado por S, e G representa o conjunto de valores adulterados dentro de todo o conjunto de dados sob estudo.

Para simplificar a análise, usou-se uma medida de desempneho que combina os valores de θ e ζ em um único número, que é conhecida como medida-F (LANTZ, 2013). A Equação 5.22 mostra como calcular a medida-F, essa medida está positivamente associada ao a eficácia do método avaliado.

$$F = \frac{2 \times \theta \times \zeta}{\theta + \zeta} \tag{5.22}$$

5.4.7 Resultados

O desempenho do mecanismo proposto neste trabalho foi medido através de 2 experimentos. Esses experimentos foram elaborados usando linguagem C do programa MATLAB®. A semente para gerar número aleatórios foi o número 5, escolhido de forma arbitrária. Tais testes foram utilizados para verificar a capacidade do mecanismo em determinar um subconjunto de elementos adulterados com os modelos de ataque propostos.

5.4.7.1 Verificação da eficácia da técnica proposta diante do modelo de ataque de clonagem de medições

Neste experimento, usou-se o modelo de ataque de clonagem de medições de HC. Inicialmente, calculou-se a média das medições de HC no conjunto de dados sob estudo (63,02 10^{-6}L/L). Depois, as medições de veículos com mais de 10 anos de idade ou com mais de 144000 km percorridos foram alteradas pelo valor da média de HC - 63,02 10^{-6}L/L. O quantitativo de valores de HC alterados foi de 80 medições.

Depois do processo de contaminação do conjunto de dados, usando o procedimento descrito na subseção 4.2.3.2, calculou-se o número de grupos ótimo para se aplicar a técnica de agrupamento. Em seguida, aplicando-se a técnica de agrupamento ao conjunto de dados contaminado, determinou-se que o número de grupos ótimo para aplicação da técnica de agrupamento é 7. Por motivos de comparação, esse número de grupos foi utilizado para avaliar as estruturas de agrupamento

propostas.

5.4.7.2 Estrutura de agrupamento original

Nesta abordagem, usou-se a estrutura original para aplicação da técnica de agrupamento *k-means*. Esta estrutura considerou somente os atributos pertencentes ao conjunto de dados. A Tabela 5.13 mostra o número de elementos de cada grupo, bem como os valores de assimetria e curtose das medições de HC pertencentes a cada grupo obtido.

Os grupos 2 e 7 têm poucos elementos e podem ser considerados como anômalos, baseado na premissa de que dados legítimos pertencem a grupos grandes e densos, enquanto anomalias grupos pequenos e esparsos (CHANDOLA; BANERJEE; KUMAR, 2009). Para os grupos restantes, a Tabela 5.13 mostra que o grupo 3 é o anômalo, visto que o parâmetro de assimetria para o conjunto de medições de HC pertencentes a esse grupo possui valor negativo. O valor de curtose, neste caso, não indicou nenhum grupo como suspeito. Analisando os grupos 2, 3 e 7 constatou-se 23 valores adulterados, representando um valor de θ de 59 %, ζ de 29 %, e um valor da medida-F de 39 %.

5.4.7.3 Estrutura agregada de agrupamento com a Lei de Benford

Nesta abordagem, usou-se a estrutura agregada para aplicação da técnica de agrupamento *k-means*. Esta estrutura considerou os atributos pertencentes ao conjunto de dados mais duas colunas correspondentes ao grau de anomalia obtidos pela Lei de Benford e associados a cada elemento do conjunto de dados. A Tabela 5.14 mostra o número de elementos de cada grupo, bem como os valores de assimetria

Tabela 5.13: Número de elementos de cada grupo, valores de assimetria e curtose das medições de HC pertencentes a cada grupo após técnica de agrupamento *k-means* com uma estrutura original

Grupo	Elementos	Assimetria	Curtose
1	148	0,94	4,10
2	1	–	–
3	36	-0,94	2,05
4	74	1,90	7,67
5	134	1,65	4,86
6	131	1,35	6,14
7	2	0,00	1,00

e curtose das medições de HC pertencentes a cada grupo obtido.

Os grupos 1 e 2 têm poucos elementos e podem ser considerados como anômalos. Para os grupos restantes, a Tabela 5.14 mostra que o grupo 3 é o anômalo, visto que o parâmetro de assimetria para o conjunto de medições de HC pertencentes a esse grupo possui valor negativo. O valor de curtose, neste caso, não indicou nenhum grupo como suspeito. Analisando os grupos 1,2 e 3 constatou-se 78 valores adulterados, representando um valor de θ de 86 %, ζ de 98 %, e um valor da medida-F de 92 %. Com um valor de medida-F igual a 92 %, a técnica de agrupamento *k-means* usando a estrutura agregada com a Lei de Benford identificou mais valores adulterados do que a estrutura original. Isto aponta o alto poder da Lei de Benford em identificar resultados clonados.

5.4.7.4 Estrutura agregada de agrupamento com a distribuição estatística Gama

Nesta abordagem, usou-se a estrutura agregada para aplicação da técnica de agrupamento *k-means*. Esta estrutura considerou os atributos pertencentes ao conjunto de dados mais uma coluna correspondente ao grau de anomalia obtido

Tabela 5.14: Número de elementos de cada grupo, valores de assimetria e curtose das medições de HC pertencentes a cada grupo após técnica de agrupamento *k-means* com uma estrutura agregada com a Lei de Benford

Grupo	Elementos	Assimetria	Curtose
1	2	0,00	1,00
2	1	–	–
3	88	-3,82	15,62
4	125	2,40	8,05
5	106	1,14	3,76
6	96	1,30	5,23
7	108	1,78	7,91

pelo uso da distribuição estatística Gama como referência. A Tabela 5.15 mostra o número de elementos de cada grupo, bem como os valores de assimetria e curtose das medições de HC pertencentes a cada grupo obtido.

Os grupos 2 e 7 têm poucos elementos e podem ser considerados como anômalos. Para os grupos restantes, a Tabela 5.15 mostra que o grupo 3 é o anômalo, visto que o parâmetro de assimetria para o conjunto de medições de HC pertencentes a esse grupo possui valor negativo. O valor de curtose, neste caso, não indicou nenhum grupo como suspeito. Analisando os grupos 2, 3 e 7 constatou-se 23 valores adulterados, representando um valor de θ de 59 %, ζ de 29 %, e um valor da medida-F de 39 %. O uso da estrutura agregada com a distribuição estatística Gama obteve o mesmo desempenho da estrutura original. Assim, mostra-se que o uso do grau de anomalia tendo como referência a distribuição estatística Gama não foi efetiva contra o ataque de clonagem de resultados.

Tabela 5.15: Número de elementos de cada grupo, valores de assimetria e curtose das medições de HC pertencentes a cada grupo após técnica de agrupamento *k-means* com uma estrutura agregada com a distribuição estatística Gama

Grupo	Elementos	Assimetria	Curtose
1	148	0,94	4,10
2	1	–	–
3	36	-0,95	2,06
4	74	1,90	7,67
5	134	1,65	4,86
6	131	1,36	6,14
7	2	0,00	1,00

5.4.7.5 Estrutura agregada de agrupamento com a distribuição estatística Gama e a Lei de Benford

Nesta abordagem, usou-se a estrutura agregada para aplicação da técnica de agrupamento *k-means*. Esta estrutura considerou os atributos pertencentes ao conjunto de dados mais três colunas correspondentes ao grau de anomalia obtidos pela Lei de Benford e pela distribuição estatística Gama. A Tabela 5.16 mostra o número de elementos de cada grupo, bem como os valores de assimetria e curtose das medições de HC pertencentes a cada grupo obtido.

Os grupos 1 e 2 têm poucos elementos e podem ser considerados como anômalos. Para os grupos restantes, a Tabela 5.14 mostra que o grupo 3 é o anômalo, visto que o parâmetro de assimetria para o conjunto de medições de HC pertencentes a esse grupo possui valor negativo. O valor de curtose, neste caso, não indicou nenhum grupo como suspeito. Analisando os grupos 1, 2 e 3 constatou-se 78 valores adulterados, representando um valor de θ de 86 %, ζ de 98 %, e um valor da medida-F de 92 %. O uso da estrutura agregada com a distribuição estatística Gama e a Lei de Benford obteve o mesmo desempenho da aplicação do procedimento proposto com a estrutura agregada considerando apenas a Lei de Benford. Esta constata-

ção confirma a pouca efetividade do uso da distribuição estatística Gama contra o ataque de clonagem de resultados.

Tabela 5.16: Número de elementos de cada grupo, valores de assimetria e curtose das medições de HC pertencentes a cada grupo após técnica de agrupamento *k-means* com uma estrutura agregada com a distribuição estatística Gama e a Leide Benford

Grupo	Elementos	Assimetria	Curtose
1	2	0,00	1,00
2	1	–	–
3	88	-3,82	15,62
4	125	2,40	8,05
5	106	1,14	3,76
6	96	1,30	5,23
7	108	1,78	7,91

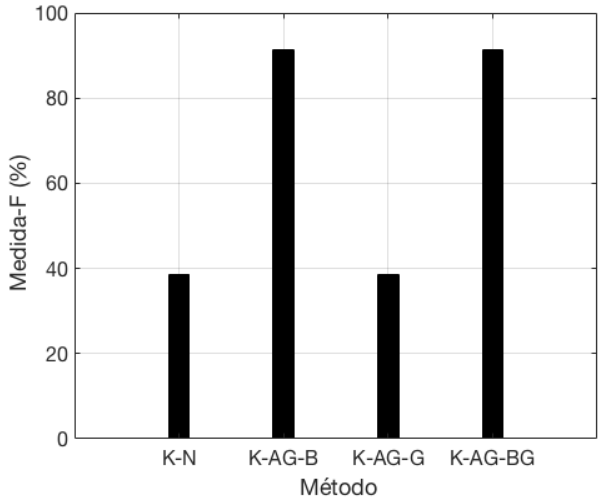


Figura 5.10: Comparação dos valores da medida-F obtidos para cada abordagem aplicada contra o modelo de ataque de clonagem de resultados, onde 'K-N' se refere a *k-means* e estrutura original; 'K-AG-B', *k-means* e estrutura agregada com a Lei de Benford; 'K-AG-B', *k-means* e a estrutura agregada com a distribuição estatística Gama; 'K-AG-BG', *k-means* e a estrutura agregada com a distribuição estatística Gama e a Lei de Benford

A Figura 5.10 mostra os valores da medida-F obtidos para cada abordagem aplicada contra o modelo de ataque de clonagem de resultados. O método mais

efetivo foi o uso da técnica de agrupamento *k-means* e a estrutura agregada com a Lei de Benford.

5.4.7.6 Verificação da eficácia da técnica proposta diante do modelo de ataque de substituição de medições por valores aleatórios

Neste experimento, usou-se o modelo de ataque de substituição de medições de HC por valores aleatórios para os mesmos 80 valores de HC escolhidos anteriormente no Experimento I. Escolheu-se aleatoriamente valores do intervalo 1 to 100 10^{-6}L/L com uma probabilidade de escolha uniforme. A intenção foi de simular o comportamento de um fraudador que deseja aprovar os veículos no teste de poluentes independente das condições dos mesmos.

Depois do processo de contaminação do conjunto de dados, usando o procedimento descrito na subseção 4.2.3.2, calculou-se o número de grupos ótimo para se aplicar a técnica de agrupamento. Em seguida, aplicando-se a técnica de agrupamento ao conjunto de dados contaminado, determinou-se que o número de grupos ótimo para aplicação da técnica de agrupamento é 8. Por motivos de comparação, esse número de grupos foi utilizado para avaliar as estruturas de agrupamento propostas.

5.4.7.7 Estrutura de agrupamento original

Nesta abordagem, usou-se a estrutura original para aplicação da técnica de agrupamento *k-means* contra ao modelo de ataque de substituição aleatória de valores de HC. Esta estrutura considerou somente os atributos pertencentes ao conjunto de dados. A Tabela 5.17 mostra o número de elementos de cada grupo, bem como

Tabela 5.17: Número de elementos de cada grupo, valores de assimetria e curtose das medições de HC pertencentes a cada grupo após técnica de agrupamento *k-means* com uma estrutura original

Grupo	Elementos	Assimetria	Curtose
1	105	1,32	5,43
2	85	0,97	4,01
3	1	–	–
4	144	1,75	5,44
5	2	0,00	1,00
6	36	0,31	1,79
7	103	0,97	3,93
8	50	1,72	6,50

os valores de assimetria e curtose das medições de HC pertencentes a cada grupo obtido.

Os grupos 3 e 5 têm poucos elementos e podem ser considerados como anômalos. Para os grupos restantes, a Tabela 5.17 mostra que o grupo 6 é o anômalo, visto que possui os menores valores para os parâmetros de assimetria e curtose com respeito ao conjunto de medições de HC pertencentes a esse grupo. Analisando os grupos 3, 5 e 6 constatou-se 23 valores adulterados, representando um valor de θ de 59 %, ζ de 29 %, e um valor da medida-F de 39 %.

5.4.7.8 Estrutura agregada de agrupamento com a Lei de Benford

Nesta abordagem, usou-se a estrutura agregada para aplicação da técnica de agrupamento *k-means*. Esta estrutura considerou os atributos pertencentes ao conjunto de dados mais duas colunas correspondentes ao grau de anomalia obtidos pela Lei de Benford e associados a cada elemento do conjunto de dados. A Tabela 5.18 mostra o número de elementos de cada grupo, bem como os valores de assimetria

e curtose das medições de HC pertencentes a cada grupo obtido.

Os grupos 3 e 6 têm poucos elementos e podem ser considerados como anômalos. Para os grupos restantes, a Tabela 5.18 mostra que o grupo 2 é o anômalo, visto que o parâmetro de assimetria para o conjunto de medições de HC pertencentes a esse grupo possui valor negativo. O valor de curtose, neste caso, não indicou nenhum grupo como suspeito. Analisando os grupos 2, 3 e 6 constatou-se 18 valores adulterados, representando um valor de θ de 17 %, ζ de 22 %, e um valor da medida-F de 19 %. Com um valor de medida-F igual a 19 %, a técnica de agrupamento *k-means* usando a estrutura agregada com a Lei de Benford identificou menos valores adulterados do que a estrutura original. Isto indica o fraco desempenho da Lei de Benford em identificar resultados adulterados de forma aleatória usando uma distribuição uniforme.

Tabela 5.18: Número de elementos de cada grupo, valores de assimetria e curtose das medições de HC pertencentes a cada grupo após técnica de agrupamento *k-means* com uma estrutura agregada com a Lei de Benford

Grupo	Elementos	Assimetria	Curtose
1	27	0,81	5,62
2	106	-0,36	2,20
3	1	–	–
4	94	3,20	12,74
5	121	1,42	7,04
6	2	0,00	1,00
7	128	3,49	25,15
8	47	0,76	2,08

5.4.7.9 Estrutura agregada de agrupamento com a distribuição estatística Gama

Nesta abordagem, usou-se a estrutura agregada para aplicação da técnica de agrupamento *k-means*. Esta estrutura considerou os atributos pertencentes ao

conjunto de dados mais uma coluna correspondente ao grau de anomalia obtido pelo uso da distribuição estatística Gama como referência. A Tabela 5.19 mostra o número de elementos de cada grupo, bem como os valores de assimetria e curtose das medições de HC pertencentes a cada grupo obtido.

Os grupos 1, 3, 6, e 8 têm poucos elementos e podem ser considerados como anômalos. Para os grupos restantes, a Tabela 5.19 mostra que o grupo 5 é o anômalo, visto que possui os menores valores para os parâmetros de assimetria e curtose com respeito ao conjunto de medições de HC pertencentes a esse grupo. Analisando os grupos 1, 3, 5, 6 e 8 constatou-se 23 valores adulterados, representando um valor de θ de 56 %, ζ de 29 %, e um valor da medida-F de 38 %. O uso da estrutura agregada com a distribuição estatística Gama obteve desempenho similar ao obtido pela estrutura original. Assim, mostra-se que o uso do grau de anomalia tendo como referência apenas a distribuição estatística Gama não foi efetiva contra o ataque de substituição aleatória de resultados de resultados, embora tenha indicado um desempenho melhor que a estrutura agregada com a Lei de Benford.

Tabela 5.19: Número de elementos de cada grupo, valores de assimetria e curtose das medições de HC pertencentes a cada grupo após técnica de agrupamento *k-means* com uma estrutura agregada com a distribuição estatística Gama

Grupo	Elementos	Assimetria	Curtose
1	1	–	–
2	162	1,64	5,02
3	1	–	–
4	182	1,84	8,77
5	37	0,25	1,76
6	1	–	–
7	141	1,30	5,52
8	1	–	–

5.4.7.10 Estrutura agregada de agrupamento com a distribuição estatística Gama e a Lei de Benford

Nesta abordagem, usou-se a estrutura agregada para aplicação da técnica de agrupamento *k-means*. Esta estrutura considerou os atributos pertencentes ao conjunto de dados mais três colunas correspondentes ao grau de anomalia obtidos pela Lei de Benford e pela distribuição estatística Gama. A Tabela 5.20 mostra o número de elementos de cada grupo, bem como os valores de assimetria e curtose das medições de HC pertencentes a cada grupo obtido.

Os grupos 3 e 8 têm poucos elementos e podem ser considerados como anômalos. Para os grupos restantes, a Tabela 5.20 mostra que o grupo 7 é o anômalo, visto que o parâmetro de assimetria para o conjunto de medições de HC pertencentes a esse grupo possui valor negativo. O valor de curtose, neste caso, não indicou nenhum grupo como suspeito. Analisando os grupos 3, 7 e 8 constatou-se 26 valores adulterados, representando um valor de θ de 70 %, ζ de 33 %, e um valor da medida-F de 45 %. Com um valor de medida-F igual a 45 %, a técnica de agrupamento *k-means* usando a estrutura agregada com a Lei de Benford e com a distribuição estatística Gama identificou mais valores adulterados do que a estrutura original. Esta constatação indica que a melhor abordagem para identificar valores adulterados contra o modelo de ataque de substituição aleatória de valores, neste caso, é usando uma estrutura agregada mista com com a Lei de Benford e com a distribuição estatística Gama.

A Figura 5.11 mostra os valores da medida-F obtidos para cada abordagem aplicada contra o modelo de ataque de substituição aleatória de resultados. O método mais efetivo foi o uso da técnica de agrupamento *k-means* e a estrutura agregada com a Lei de Benford e a distribuição estatística Gama.

Tabela 5.20: Número de elementos de cada grupo, valores de assimetria e curtose das medições de HC pertencentes a cada grupo após técnica de agrupamento *k-means* com uma estrutura agregada com a distribuição estatística Gama e a Leide Benford

Grupo	Elementos	Assimetria	Curtose
1	103	1,28	6,14
2	122	2,37	7,56
3	1	–	–
4	112	0,73	3,59
5	13	1,60	4,65
6	139	0,25	2,45
7	34	-0,05	1,82
8	2	0	1

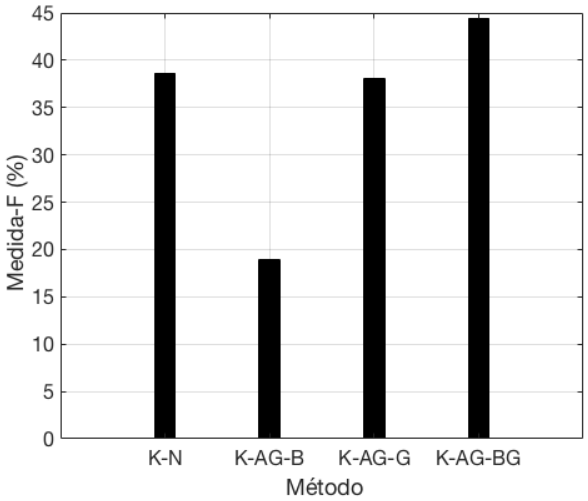


Figura 5.11: Comparação dos valores da medida-F obtidos para cada abordagem aplicada contra o modelo de ataque de substituição aleatória de resultados, onde 'K-N' se refere a *k-means* e estrutura original; 'K-AG-B', *k-means* e estrutura agregada com a Lei de Benford; 'K-AG-B', *k-means* e a estrutura agregada com a distribuição estatística Gama; 'K-AG-BG', *k-means* e a estrutura agregada com a distribuição estatística Gama e a Lei de Benford

Cabe destacar que quanto ao ataque de clonagem de dados há indicativos que a Lei de Benford pode ser melhor empregada do que o uso da distribuição estatística Gama na análise de resultados de emissões de poluentes. De outro lado, quando

experimentou-se o ataque de edição aleatória de dados a estrutura agregada da Lei de Benford e a distribuição estatística Gama se mostrou mais eficaz. Por fim, constatou-se que o uso do parâmetro de assimetria da distribuição estatística de medições de HC foi mais eficaz que o parâmetro de curtose no processo de identificação de grupos anômalos.

5.5 Estudo de caso 5

Neste estudo de caso, avalia-se a eficácia do método rápido proposto para detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade usando filmagens de seus serviços. Além disso, o tempo de processamento do método proposto é comparado com o tempo gasto por uma analista na análise desses vídeos.

5.5.1 Conjunto de dados

O conjunto de dados neste estudo de caso possui 30 vídeos reais contendo atividades relacionadas ao teste de faróis em organismos acreditados em inspeção de segurança veicular. Esses vídeos foram coletados entre 2015 e 2016, o teste de faróis foi realizado usando mesmo protocolo e com posicionamento de câmera similar. Todos os vídeos possuem formato mp4 e RGB24. A média de duração desses vídeos é de 1 min 36 s.

A Tabela 5.21 descreve o do conjunto de dados considerado neste estudo de caso. Um especialista em organismo de inspeção acreditado em segurança veicular classificou os vídeos quanto seu atendimento ao protocolo de teste. Para efeitos de validação do método proposto, considera-se neste trabalho que os testes em que a or-

ganização acreditada não seguiu o protocolo foram realizados de forma intencional, caracterizando-se assim casos fraudulentos. Devido a requisitos de confidencialidade, as organizações envolvidas não podem ser mencionadas, nem imagens de suas instalações e de seu pessoal podem ser mostradas.

Tabela 5.21: Descrição do conjunto de dados com vídeos de inspeção em organismos de segurança veicular

Organismo	Vídeos	Falha em seguir o protocolo?
1	V1-V21	Não
2	V22-V29	Sim, V29
3	V30	Sim, V30

5.5.2 Determinando os vídeos anômalos

Um comportamento fraudulento ocorre quando um organismo de avaliação da conformidade falha intencionalmente em seguir um protocolo. Um protocolo geralmente tem um número mínimo de passos para assegurar sua performance adequada. Assim, o número de movimentos detectados em um vídeo de um serviço de avaliação da conformidade pode indicar suspeitas de não cumprimento do protocolo do serviço. Os movimentos detectados podem ser ações realizadas pelo operadores de equipamentos, objetos sendo transladados ou outra ação que expresse diferenciação entre quadros de uma filmagem.

No processo de detecção de movimentos para cada vídeo, a técnica de diferença temporal (LIPTON; FUJIYOSHI; PATIL, 1998) e o filtro homomórfico (TOTH; AACH; METZLER, 2000), (RADKE et al., 2005) são utilizados. A diferença entre a componentes de reflectância dos quadros estatisticamente diferentes são usadas para verificar regiões onde há movimento. Usando a diferença absoluta entre dois quadros estatisticamente diferentes, aplica-se uma função limiar para determinar mudanças. Para cada vídeo, o número de mudanças detectadas são re-

gistradas. A técnica de diferença temporal é utilizada devido ao seu baixo custo computacional, favorecendo o estabelecimento do método rápido de monitoramento de organismos. O processamento dos vídeos é feito externamente ao sistema de captação das filmagens.

Após a diferença absoluta entre dois quadros consecutivos ser obtida, um função limiar é usada para determinar mudanças. Uma imagem de movimento M_n pode ser extraída através da operação

$$M_n(u,v) = \begin{cases} I_n(u,v),\ D_n(u,v) \geq T \\ 0,\ D_n(u,v) < T \end{cases} \tag{5.23}$$

Para cada imagem M_n extraída do vídeo, conta-se um movimento, até que ao final do processamento do vídeo $V1$, tenha-se uma quantidade de movimentos expressa pela grandeza $MO1$. Quando todos os vídeos V forem processados, ter-se-á uma lista de quantidade de movimentos $\{MO1, MO2, ¨, MOV\}$ que podem ser ser comparados para indicação dos vídeos anômalos.

Para determinar os vídeos anômalos, usou-se a distância de um determinado elemento no conjunto de dados aos seus *k-nearest neighbors*. A técnica de *k-nearest neighbors* determina, dentro de um conjunto de dados, os k elementos mais similares a um determinado elemento no conjunto, sendo que k deve ser estabelecido antecipadamente. O valor k pode ser estimado pela raiz quadrada do número de elementos no conjunto de dados (LANTZ, 2013). Os elementos com maior distância para seus *k-nearest neighbors* serão considerados anômalos (AGGARWAL, 2013).

Para medir a similaridade entre vizinhos, usou-se a distância de Manhattan. Sejam $j = (x_{j1}, x_{j2}, \cdots, x_{jp})$ e $k = (x_{k1}, x_{k2}, \cdots, x_{kp})$ dois objetos descritos por p atributos númericos. A distância de Manhattan entre esses dois objetos j e k é

definida por $d(j,k) = |x_{j1} - x_{k1}| + |x_{j2} - x_{k2}| + \cdots + |x_{jp} - x_{kp}|$(HAN; PEI; KAMBER, 2011).

Finalmente, o grau de anomalia de cada vídeo pode ser estabelecido pelo somatório das distâncias de Manhattan dos k-zinhos mais próximos. Os elementos anômalos podem ser determinados por uma função de limiar ou por um número fixo dos elementos como maior grau de anomalia (CHANDOLA; BANERJEE; KUMAR, 2009).

5.5.3 Resultados

MATLAB®foi utilizado na implementação do procedimento proposto para identificar possíveis serviços fraudulentos em vídeos. Todos os quadros dos vídeos foram convertidos para suas representação em escala de cinza antes da avaliação de quais imagens seriam estatisticamente diferentes. Para o uso da técnica de *k-nearest neighbors*, usou-se k = 5, que corresponde a um valor aproximado da raiz quadrada do número de medidas obtidas do conjunto de dados (30 medições de quantidade de movimentos).

Figura 5.12 mostra o grau de anomalia de cada vídeo analisado com relação ao número de movimento detectados nesses vídeos pelo método de análise rápida de filmagens. Os dados na figura indicam que uma estimativa razoável para o número de vídeos anômalos igual a 3, visto que pode-se notar três vídeos com grau de anomalia substancialmente diferente dos demais vídeos. Neste caso, os três vídeos são V29, V30 e V15. Os vídeos V29 e V30 são os mais suspeitos de não se ter o protocolo completamente seguido, uma vez que possuem uma quantidade de movimentos detectados bem menor que os demais vídeos. De outro lado, tem-se o vídeo V15 onde o inspetor da organização acreditada refez algumas etapas do teste

para assegurar seu completo cumprimento, desta forma esse vídeo contemplou um número bem maior de movimentos detectados que os demais vídeos.

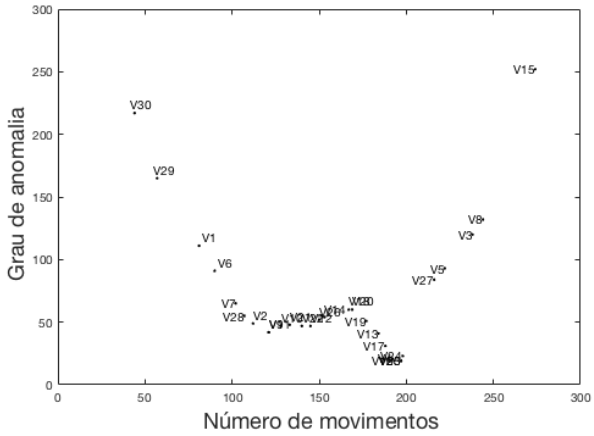


Figura 5.12: Grau de anomalia de cada vídeo analisado com relação ao número de movimento detectados nesses vídeos

Para comparar o desempenho do método proposto quanto ao tempo necessário para se analisar um determinado conjunto de vídeos, usou-se um computador portátil com 2.5 GHz Intel Core i5, 8 GB 1600 MHz DDR3, e sistema MAC OSX.

A Figura 5.13 mostra o tempo de processamento do método proposto e o tempo necessário para o processamento dos vídeos usando método tradicional. O método proposto levou 30 minutos para analisar os 30 vídeos existentes no conjunto de dados. Após a identificação dos três vídeos anômalos, uma analista levaria 4 minutos para assistí-los podendo confirmar algum caso de fraude. Assim, com o método proposto, gastaria-se um tempo de 34 minutos para processar os vídeos do conjunto de dados.

Por outro lado, usando o método tradicional em que o analista deve assistir todos os 30 vídeos minuto a minuto, gastaria-se no mínimo 41 minutos que o tempo total de duração de todos os vídeos considerados neste estudo de caso. Além disso,

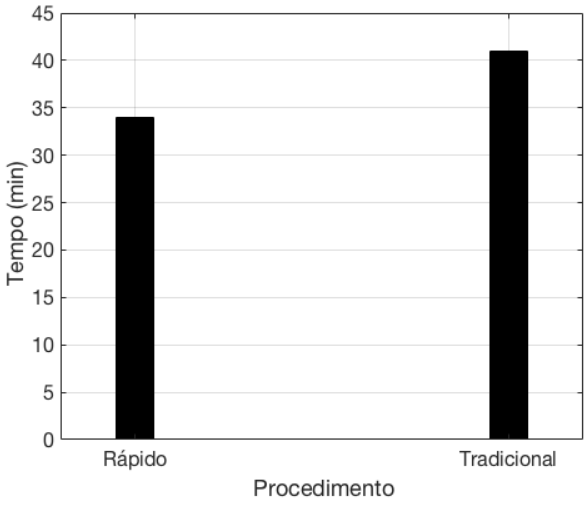


Figura 5.13: Comparação entre o tempo de processamento do método proposto e o tempo necessário para o processamento dos vídeos usando método tradicional

para realizar esta tarefa, o analista deve focar sua atenção constantemente nos vídeos para não perder nenhum detalhe. Ao contrário de quando usa o método proposto, onde o analista pode realizar outras tarefas de auditoria enquanto o método rápido processa os vídeos considerados para estudo. Isto representa um ganho de tempo e recursos.

5.6 Estudo de caso 6

Neste estudo de caso, avalia-se a eficácia de um método proposto para detecção de possíveis serviços fraudulentos em um organismo de avaliação da conformidade usando retroalimentação. Devido aos poucos exemplos de serviços de inspeção com falha, decidiu-se adotar uma abordagem alternativa de se avaliar novas sequências usando sequências legítimas como referências.

5.6.1 Conjunto de dados

O conjunto de dados neste estudo de caso possui 30 vídeos reais contendo atividades relacionadas ao teste de faróis em organismos acreditados em inspeção de segurança veicular. Esses vídeos foram coletados entre 2015 e 2016, o teste de faróis foi realizado usando mesmo protocolo e com posicionamento de câmera similar. Todos os vídeos possuem formato mp4 e RGB24. A média de duração desses vídeos é de 1 min 36 s.

A Tabela 5.22 descreve o do conjunto de dados considerado neste estudo de caso. Um especialista em organismo de inspeção acreditado em segurança veicular classificou os vídeos quanto seu atendimento ao protocolo de teste. Para efeitos de validação do método proposto, considera-se neste trabalho que os testes em que a organização acreditada não seguiu o protocolo foram realizados de forma intencional, caracterizando-se assim casos fraudulentos. Devido a requisitos de confidencialidade, as organizações envolvidas não podem ser mencionadas, nem imagens de suas instalações e de seu pessoal podem ser mostradas.

Tabela 5.22: Descrição do conjunto de dados com vídeos de inspeção em organismos de segurança veicular

Organismo	Vídeos	Falha em seguir o protocolo?
1	V1-V21	Não
2	V22-V29	Sim, V29
3	V30	Sim, V30

5.6.2 Resultados

Nos experimentos realizados, primeiramente, estabeleceu-se o cálculo dos histogramas orientados de fluxo ótico para as ações em cada vídeo. Em seguida,

aplicou-se a técnica de alinhamento local para comparar um novo subconjunto de vídeos usando as suas sequências de histogramas orientados de fluxo ótico com as sequências de referência. O objetivo é verificar a similaridade dos elementos de teste com as sequências de referência para os serviços legítimos. Os experimentos foram realizados usando o MATLAB ®.

5.6.3 Extraindo o histograma de fluxo ótico de cada vídeo

Para o cálculo do fluxo ótico de cada cena, devido a sua simplicidade e baixo custo computacional, usou-se o método de Lucas-Kanade (LUCAS, 1986). O método de Lucas-Kanade assume que o deslocamento do conteúdo de uma imagem entre dois quadros próximos é pequeno e aproximadamente constante dentro de uma vizinhança de pixels. Assim, a equação de fluxo ótico pode ser considerada para todos os pixels dentro de uma janela centrada em um pixel p. Deste modo, tem-se

$$\begin{cases} I_u(q_1)\dot{u} + I_v(q_1)\dot{v} = -I_t(q_1) \\ I_u(q_2)\dot{u} + I_v(q_2)\dot{v} = -I_t(q_2) \\ \vdots \\ I_u(q_w)\dot{u} + I_v(q_w)\dot{v} = -I_t(q_w) \end{cases} \tag{5.24}$$

onde $q_1, q_2, \cdots, q_w$ são os pixels dentro da janela w considerada, I_u, I_v, I_t são as derivadas parciais com relação a posição u, v e com relação ao tempo t avaliadas nos pixels da janela considerada no cálculo do fluxo ótico.

O sistema de equações mostrado em 5.27 pode ser escrito na forma matricial $Ax = b$. Onde,

$$A = \begin{bmatrix} I_u(q_1) & I_v(q_1) \\ I_u(q_2) & I_v(q_2) \\ \vdots & \\ I_u(q_w) & I_v(q_w) \end{bmatrix} \tag{5.25}$$

$$x = \begin{bmatrix} \dot{u} \\ \dot{v} \end{bmatrix} \tag{5.26}$$

$$b = \begin{bmatrix} -I_t(q_1) \\ -I_t(q_2) \\ \vdots \\ -I_t(q_w) \end{bmatrix} \tag{5.27}$$

Pelo princípio dos mínimos quadrados, o sistema $Ax = b$ pode ser resolvido da seguinte forma

$$Ax = b$$

$$A^T Ax = A^T b$$

$$x = (A^T A)^{-1} A^T b$$

De posse dos valores correspondentes ao fluxo ótico, constrói-se, para cada cena no vídeo, o histogram orientado de fluxo ótico. Em (CHAUDHRY et al., 2009), os autores constataram que o histograma com 30 intervalos foi suficiente para bons

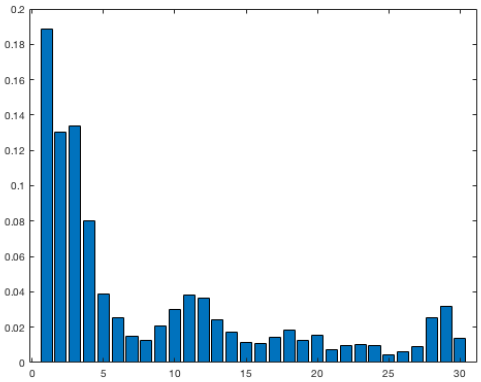
resultados, desta forma, neste trabalho, também usa-se o mesmo valor de intervalos para constituir os histogramas nos experimentos desenvolvidos. Para o cálculo do histograma orientado considerou-se apenas o fluxo ótico dos objetos em movimento, analogamente ao que foi feito em (CUTLER; TURK, 1998).

No processo de detecção de movimentos para cada vídeo, a técnica de diferença temporal (LIPTON; FUJIYOSHI; PATIL, 1998) e o filtro homomórfico (TOTH; AACH; METZLER, 2000), (RADKE et al., 2005) são utilizados. A diferença entre a componentes de reflectância dos quadros estatisticamente diferentes são usadas para verificar regiões onde há movimento. Usando a diferença absoluta entre dois quadros estatisticamente diferentes, aplica-se uma função limiar para determinar mudanças.

A Figura 5.14 mostra um exemplo de histograma orientado de fluxo ótico de uma cena captada em um dos vídeos que compõe o conjunto de dados desse estudo. Essa figura é composta da silhueta captada em uma cena - Figura 5.14(a), do fluxo ótico calculado para as partes em movimento - Figura 5.14(b), e o histograma orientado de fluxo ótico calculado para os vetores de fluxo encontrados - Figura 5.14(c). Cabe destacar, que os vetores de fluxo foram aumentados para possibilitar a melhor visualização deles, sendo que nem todos os vetores calculados são mostrados.

(a) Silhueta

(b) Fluxo ótico



(c) Histograma orientado de fluxo ótico

Figura 5.14: Ilustração do histograma orientado de fluxo ótico de uma cena captada em um dos vídeos que compõe o conjunto de dados desse estudo.

5.6.4 Determinando a correspondência entre duas ações

No contexto de alinhamento de sequências genéticas, existem símbolos bem definidos, por exemplo, as bases de DNA - A, G, T e C. Esses elementos podem ser comparados facilmente para se determinar correspondências, ocorrência de símbolos

iguais, ou não-correspondências, ocorrência de elementos diferentes em uma mesma posição.

Por outro lado, nesse estudo de caso, tem-se uma sequência de ações de um determinado ensaio representada por uma sequência de histogramas. Assim, a forma de se determinar a correspondência entre elementos será diferente do método usado no alinhamento de sequências genéticas. Para determinar uma correspondência entre histogramas, avalia-se o grau de similaridade entre eles através de uma medida de distância. Se a distância entre dois histogramas estiver dentro de um limiar d predeterminado, considera-se que há uma correspondência. Caso contrário, há uma não correspondência. Neste estudo de caso, usa-se a distância Euclidiana entre os histogramas a serem comparados para se medir seu grau de similaridade. Esse método visa compensar o fato que as silhuetas obtidas nas cenas podem ter tamanhos diferentes que, por sua vez, podem causar histogramas ligeiramente diferentes, assim um limiar de aceitação é razoável.

5.6.5 Escolhendo o sistema de pontuação para alinhamento das sequências

Quando se faz alinhamento de sequências genéticas, é comum se utilizar de matrizes de substituição como funções de pontuação (MCGHEE, 2007). Essa matriz atribui pontos diferentes para as correspondências e não-correspondências, dados estes retirados de estudos estatísticos de vários conjuntos de dados. Por exemplo, a matriz de substituição BLOSUM 50 atribui o valor -2 para a não-correspondência entre o resíduo de proteína "R" com o resíduo "D", enquanto a correspondência entre o resíduo "R" com resíduo "R" receberia uma pontuação de +7.

Neste estudo de caso, tendo em vista que não há uma matriz de substituição

que pontue ações de ensaio de avaliação da conformidade, a função de pontuação de correspondências seguirá os seguintes critérios:

a) quando houver uma correspondência, atribui-se um valor de pontuação igual a +1, pois, neste caso, têm-se ações similares.

b) quando houver uma não-correspondência, atribui-se o valor -1, de modo que o sistema seja incentivado a não relacionar ações diferentes.

c) quando for inserida uma lacuna, deve-se atribuir o valor 0 como incentivo, uma vez que não há uma correspondência e nem uma não-correspondência.

Para todos os experimentos nas próximas subseções, seguiu-se o sistema de pontuação acima.

5.6.6 Comparando sequências de referência com sequências legítimas e fraudulentas

Dentro das cinco sequências legítimas descritas na Tabela 5.22, 25 sequências foram escolhidas como sendo sequências de referência, sendo denominadas de S_{l1}, S_{l2}, S_{l3} e S_{l7} até S_{l28}. As outras três sequências legítimas (S_{l4}, S_{l5}, S_{l6}) e as duas fraudulentas (S_{f29}, S_{f30}) formularam o conjunto de teste. A pontuação de similaridade foi dada como sendo a maior pontuação obtida para a melhor região alinhada pela técnica de Smith-Waterman (SMITH; WATERMAN, 1981).

A Figura 5.15 mostra a comparação entre sequências de referência e outras sequências legítimas e fraudulentas. Nota-se que para sequência legítima S_{l6} existem alguns pontos de similaridade próximos aos valores de similaridade atribuídos as

sequências fraudulentas. Isso pode ser explicado pelo pequeno valor de limiar na decisão de correspondência dos histogramas, que permitiu o alinhamento de regiões pequenas. Assim, o uso de uma limiar muito restrito não é recomendado.

Se for utilizada a somatória das pontuações com relação às sequências de referências como indicador, nota-se que as sequências fraudulentas possuem um total de pontos menor que as sequências legítimas, conforme mostrado na Figura 5.16. Este fato dá indícios de que tendo um conjunto legítimo de referência, e usando a técnica de Smith-Waterman, pode-se ter casos suspeitos de fraude nos serviços que tenham as menores pontuações de alinhamento.

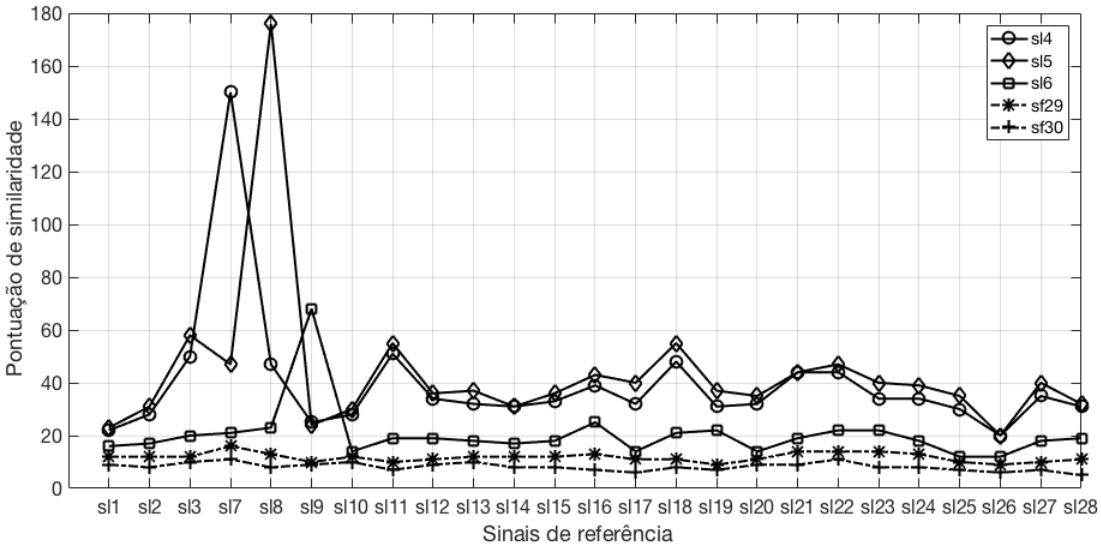


Figura 5.15: Pontuação de similaridade entre uma assinaturas legítimas (sl4, sl5 e sl6) e fraudulentas(sf29 e sf30) com relação a assinaturas legítimas de referência sendo limiar de correspondência $d = 0.1$.

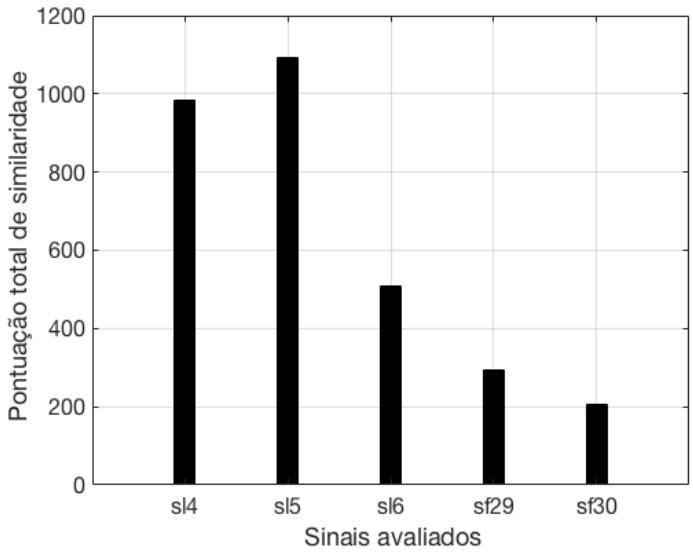


Figura 5.16: Pontuação total de similaridade entre uma assinaturas legítimas (sl4, sl5 e sl6) e fraudulentas(sf29 e sf30) com relação a assinaturas legítimas de referência sendo limiar de correspondência $d = 0.1$.

A Figura 5.17 mostra a comparação entre sequências de referência e outras sequências legítimas e fraudulentas. Nota-se que as sequências legítimas e fraudulentas já possuem uma melhor separabilidade com o limiar de correspondência $d = 0.2$. Ainda na Figura 5.18, percebe-se que as sequências fraudulentas possuem o menor valor de pontuação total de similaridade.

A Figura 5.19 mostra a comparação entre sequências de referência e outras sequências legítimas e fraudulentas. Nota-se que com o aumento do limiar de correspondência para $d = 0.3$, as sequências legítimas e fraudulentas aumentaram sua separabilidade. Porém, não se recomenda aumentar esse valor de limiar indefinidamente, visto que quanto mais permissivo ele for, maior é a chance de se fazer a correspondência entre ações que sejam bem diferentes entre si. Ainda na Figura 5.20, percebe-se que as sequências fraudulentas possuem o menor valor de pontuação total de similaridade. A investigação limitou-se a uma pequena faixa de valores

no que se refere o limiar de decisão d, pois aumentar esse limiar indefinidamente ocasionará a correspondência de atividades bem diferentes entre si.

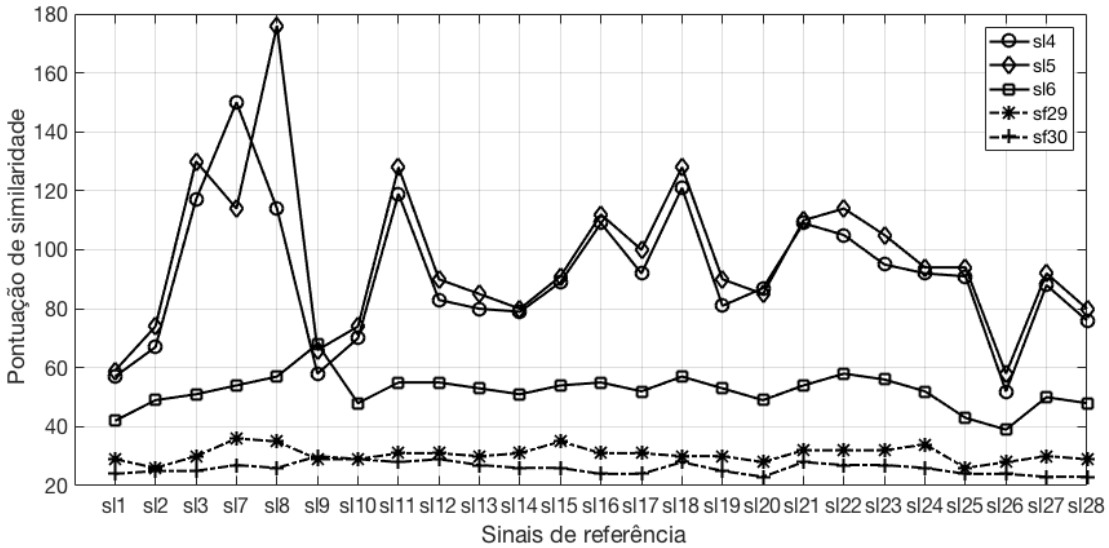


Figura 5.17: Pontuação de similaridade entre uma assinaturas legítimas (sl4, sl5 e sl6) e fraudulentas(sf29 e sf30) com relação a assinaturas legítimas de referência sendo limiar de correspondência $d = 0.2$.

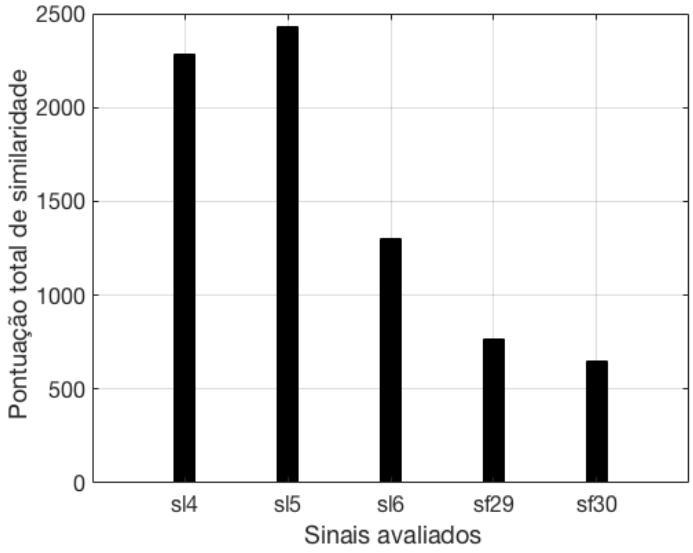


Figura 5.18: Pontuação total de similaridade entre uma assinaturas legítimas (sl4, sl5 e sl6) e fraudulentas(sf29 e sf30) com relação a assinaturas legítimas de referência sendo limiar de correspondência $d = 0.2$.

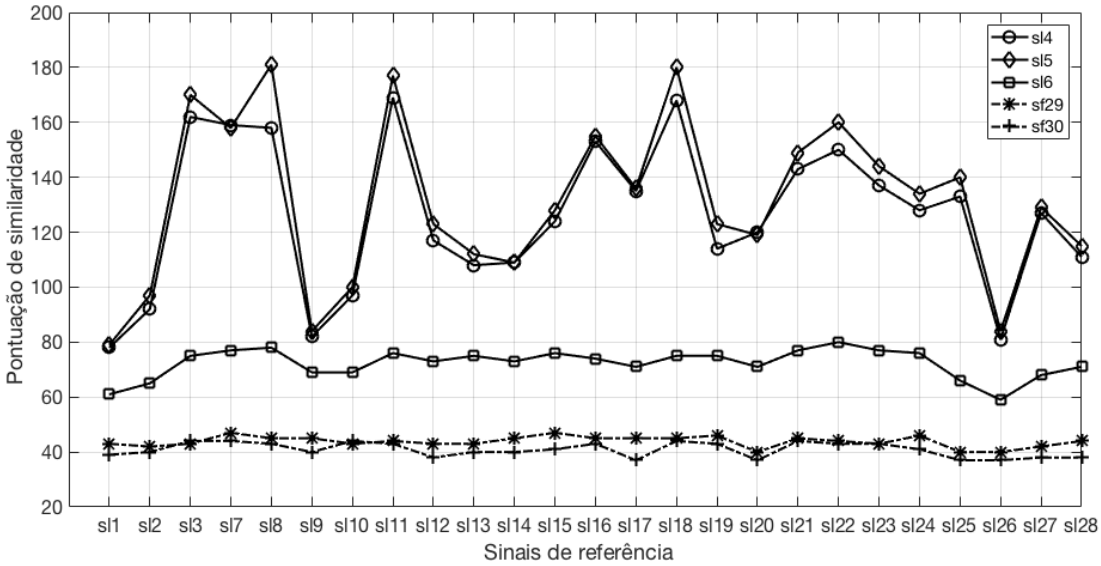


Figura 5.19: Pontuação de similaridade entre uma assinaturas legítimas (sl4, sl5 e sl6) e fraudulentas(sf29 e sf30) com relação a assinaturas legítimas de referência sendo limiar de correspondência $d = 0.3$.

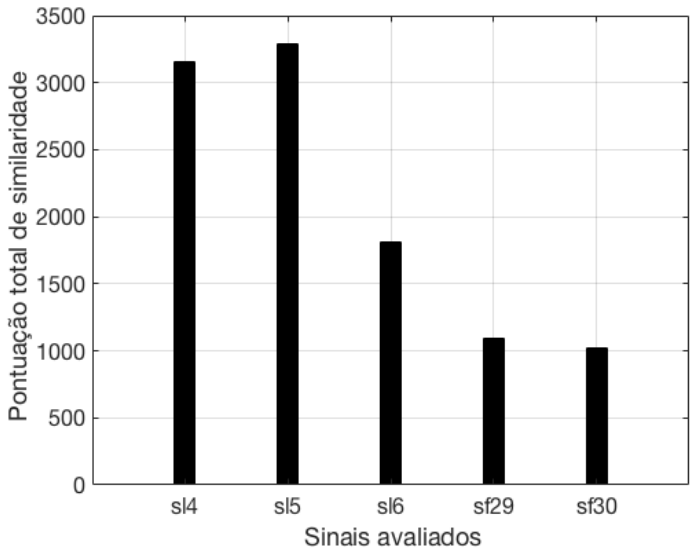


Figura 5.20: Pontuação total de similaridade entre uma assinaturas legítimas (sl4, sl5 e sl6) e fraudulentas(sf29 e sf30) com relação a assinaturas legítimas de referência sendo limiar de correspondência $d = 0.3$.

5.7 Resumo

Neste capítulo, vários experimentos foram conduzidos para validar os métodos que compõem o arcabouço proposto. Verificou-se que o arcabouço proposto pode indicar possíveis serviços fraudulentos usando técnicas de extração de conhecimento de conjunto de dados, bem como com técnicas de processamento de imagem e de alinhamento de sequências. No próximo capítulo, são apresentadas as conclusões desta tese e sugestões de trabalhos futuros.

Ademais, a combinação do método de Bootstrap com a teoria de Dempster-Shafer permite se avaliar múltiplas evidências de sintomas de fraude, ao invés de analisar apenas um parâmetro como mostrado nos trabalhos levantados de comparação de centrais de exames clínicos. Além disso, a utilização de estrutura agregada

dos valores originais com seus respectivos graus de anomalia permitiu o estabelecimento de uma nova abordagem para agrupamento de dados, diferentemente das abordagens de agrupamento utilizadas na detecção de entrevistas fabricadas conforme mostrado anteriormente. Por fim, diferente das técnicas utilizadas na detecção de anomalias usando sistema de vigilância mostradas anteriormente, como por exemplo a detecção das fraudes em supermercado, o método proposto indica uma forma de aumentar a velocidade de processamento dos vídeos descartando quadros estatisticamente similares.

6 CONCLUSÃO E TRABALHOS FUTUROS

Neste trabalho, apresentou-se uma proposta de um arcabouço para monitoramento de organismos de avaliação da conformidade. Foram discutidos os métodos para comparação de resultados entre empresas de avaliação da conformidade e para seleção de serviços de avaliação da conformidades potencialmente fraudulentos.

Observou-se que a combinação do método de Bootstrap e a teoria de Dempster-Shafer contribuiu para identificação de casos de fraude na área de inspeção de segurança veicular. Sendo que, a variabilidade de medições e a preferência por dígitos se mostraram evidências eficazes na detecção de possíveis dados fraudulentos.

Além disso, o uso mineração de dados tem um alto potencial para detecção de fraudes no sistema inspeções na área de equipamentos que transportam produtos perigosos no Brasil. Tendo em vista que a aplicação da rede neural de LVQ permitiu classificar organismos de inspeção como legítimos e fraudulentos. Em um cenário idealizado, a técnica aplicada conseguiu identificar com sucesso a maioria dos casos apresentados.

Somando-se a isso, a aplicação do Processo de Decisão de Markov juntamente com a Lei de Benford possibilitou a seleção de um subconjunto de dados com suspeita de fraude. Mostrou-se que este tipo de mecanismo pode auxiliar os avaliadores da CGCRE/Inmetro a identificar dados suspeitos de fraude durante as avaliações de supervisão dos organismos acreditados em segurança veicular.

Por sua vez, e tendo em vista os poucos exemplos de conjuntos de dados com casos fraudulentos, algumas formas de se adulterar os resultados de ensaios

realizados foram modeladas. Essa modelagem permitiu a validação da proposta de aplicação de mineração de dados em conjunto com a Lei de Benford e estatística descritiva. Nessa aplicação notou-se que a Lei de Benford apresentou-se com desempenho forte quanto ao ataque de clonagem de medições; e no contexto de emissões veiculares, a estatística de assimetria foi mais efetiva na indicação de grupos anômalos.

Ainda, pôde-se avaliar a aplicação de uma técnica para análise rápida de filmagens de serviços de avaliação da conformidade com o objetivo de apontar vídeos com possíveis serviços fraudulentos.

Além do mais, o método proposto para análise rápida de filmagens se mostrou útil para estimar o número de movimentações realizadas nos ensaios registrados nas filmagens podendo levar a identificação de serviços realizados parcialmente. Embora, essa técnica consiga estimar possíveis serviços anômalos, ela tem a limitação de não conseguir identificar que tipo de etapa não foi realizada no ensaio registrado.

Em sequência, mostrou-se que há indícios de que com a utilização de técnicas de alinhamento de sequência e de posse de um conjunto legítimo serviços de referência, pode-se indicar a existência de possíveis casos de fraude nos serviços que tenham as menores pontuações de alinhamento. Além disso, cabe destacar que a utilização de técnicas aproximadas para cálculo de silhuetas e do próprio fluxo ótico pode causar a limitação do método proposto em apenas alinhar ações não sutis, como por exemplo andar, abaixar-se, carregar um equipamento entre outras.

Os estudos de caso mostraram que as técnica foram aplicadas de forma eficaz, espera-se então que com a implementação dessas técnicas no mundo real, possa-se coletar mais evidências de validação e aprimorá-las.

Por fim, o desenvolvimento tecnológico dos últimos anos tem trazido consigo novas formas de se cometer fraude, principalmente no ambiente eletrônico. Dentro desse cenário de controle de fraudes, vários desafios estão surgindo. Dentre esses desafios pode-se destacar o caráter adaptativo dos atacantes, desta forma, indica-se como trabalhos futuros no contexto de avaliação da conformidade a criação de conjuntos de dados de referência com mais exemplos de casos fraudulentos e legítimos na área de avaliação da conformidade, isto permitirá o desenvolvimento de mais modelos que possam detectar de forma eficaz novas formas de fraude e se adaptar a evolução dos adversários.

Também sugere-se a extensão do método de comparação de organismos de avaliação da conformidade que permita uma avaliação dos dados com múltiplas variáveis. No módulo de análise de serviços, convém que sejam explorados mais tipos de ensaios e fontes de informação como por exemplo fontes de áudio e sinais elétricos de equipamentos. Além de realizar comparações entre técnicas existentes na literatura, como por exemplo, comparar mais técnicas de agrupamento quando da utilização de mineração de dados para encontrar elementos anômalos.

No caso de análise de filmagens de organismos de avaliação da conformidade, também é importante buscar formas para tratar situações em que há presença de múltiplas pessoas realizando as atividades de avaliação. Bem como, também poder avaliar os registros de filmagens de câmeras em várias posições diferentes para a mesma cena. Ainda, convém se investigar técnicas que permitam o reconhecimento das ações realizadas em cada etapa do processo de avaliação da conformidade nos vídeos.

No caso de investigação automática de casos similares, convém se estudar outras formas de assinatura e técnicas de avaliação dessas assinaturas.

Além disso, outro ponto importante para os sistemas de controle de fraudes é municiá-lo com capacidade de poder predizer tendências de comportamento fraudulento. Esse tipo de ferramenta permitirá a adoção de ações preventivas.

7 PRODUÇÃO ACADÊMICA

Neste capítulo, lista-se os artigos publicados e aceitos para publicação em decorrência do desenvolvimento desta tese de doutorado:

Artigo 1 - SOUZA, R. P.; CARMO, L. F. R. C. ; PIRMEZ, L. ; BOCCARDO, D. ; MACHADO, R. C. . Redes de Kohonen para detecção de fraudes em inspeções na área de transporte de produtos perigosos. In: 7º Congresso Brasileiro de Metrologia, 2013, Ouro Preto. 7º Congresso Brasileiro de Metrologia, 2013.

Artigo 2 - SOUZA, R. P.; CARMO, L. F. R. C. ; PIRMEZ, L. . Detecção de Dados Suspeitos de Fraude em Organismos de Inspeção Acreditdados. In: XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2014, Belo Horizonte. XIV Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, 2014.

Artigo 3 - DE SOUZA, ROSEMBERGUE P.; CARMO, LUIZ F. R. C. ; PIRMEZ, LUCI . A procedure to detect suspected patterns of fraudulent behavior in vehicle emissions tests performed by an accredited inspection body. Accreditation and Quality Assurance, v. 21, p. 323-333, 2016.

Artigo 4 - DE SOUZA, ROSEMBERGUE P.; CARMO, LUIZ F. R. C. ; PIRMEZ, LUCI . An enhanced bootstrap method to detect possible fraudulent behavior in testing facilities. Accreditation and Quality Assurance, v. 22, p. 1-7, 2017.

Artigo 5 - DE SOUZA, ROSEMBERGUE P.; CARMO, LUIZ F. R. C. ; PIRMEZ, LUCI . Rapid video assessment for monitoring testing facility fraud. International Journal of Quality & Reliability Management. Aceito para publicação em 26/09/2017.

REFERÊNCIAS

ABDALLAH, A.; MAAROF, M. A.; ZAINAL, A. Fraud detection system: a survey. **Journal of Network and Computer Applications**, Oklahoma, v.68, p.90–113, jun. 2016. Elsevier.

AGGARWAL, C. C. **Outlier analysis**. 1.ed. New York: Springer Science & Business Media, 2013.

ALLAN, T.; ZHAN, J. Towards fraud detection methodologies. In: INTERNATIONAL CONFERENCE ON FUTURE INFORMATION TECHNOLOGY, 5., Busan. **Anais...** IEEE, 2010. p.1–6.

ANGELOS, E. W. S. et al. Detection and Identification of Abnormalities in Customer Consumptions in Power Distribution Systems. **IEEE Transactions on Power Delivery**, Alberta, v.26, n.4, p.2436–2442, oct. 2011. IEEE.

ARAL, K. D. et al. A prescription fraud detection model. **Computer methods and programs in biomedicine**, Taipei, v.106, n.1, p.37–46, apr. 2012. Elsevier.

ARBIB, M. A. **The handbook of brain theory and neural networks**. 2.ed. London: MIT press, 2003.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 14040** - Inspeção de segurança veicular - Veículos leves e pesados, Rio de Janeiro, 1998.

ATTALURI, S.; MCGHEE, S.; STAMP, M. Profile hidden Markov models and metamorphic virus detection. **Journal in computer virology**, Laval, v.5, n.2, p.151–169, may 2009. Springer.

BARABESI, L. et al. Goodness-of-fit testing for the Newcomb-Benford law with application to the detection of customs fraud. **Journal of Business & Economic Statistics**, New York, p.1–13, 2017. Taylor & Francis.

BARMAN, S. et al. A complete literature review on financial fraud detection applying data mining techniques. **International Journal of Trust Management in Computing and Communications**, Warsaw, v.3, n.4, p.336–359, jun. 2016. Inderscience Publishers (IEL).

BEHDAD, M. et al. Nature-Inspired Techniques in the Context of Fraud Detection. **IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)**, Prague, v.42, n.6, p.1273–1290, nov 2012.

BIN, O. A logit analysis of vehicle emissions using inspection and maintenance testing data. **Transportation Research Part D: Transport and Environment**, Ithaca, v.8, n.3, p.215–227, may 2003. Elsevier.

BIRNBAUM, B. et al. Using behavioral data to identify interviewer fabrication in surveys. In: SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, Paris. **Proceedings...** ACM, 2013. p.2911–2920.

BOLTON, R. J.; HAND, D. J. Statistical fraud detection: a review. **Statistical Science**, Piscataway, v.17, n.3, p.235–249, aug. 2002. JSTOR.

BREDL, S.; WINKER, P.; KÖTSCHAU, K. A statistical approach to detect interviewer falsification of survey data. **Survey methodology**, Ottawa, v.38, n.1, p.1–10, jun. 2012. Statistics Canada.

BRYAN, M. F. **Randomization, bootstrap and Monte Carlo methods in biology**. 3.ed. Boca Raton: CRC Press, 2006.

BUYSE, M. et al. The role of biostatistics in the prevention, detection and treatment of fraud in clinical trials. **Statistics in Medicine**, Boston, v.18, n.24, p.3435–51, dec 1999.

CAMOSSI, E.; DIMITROVA, T.; TSOIS, A. Detecting anomalous maritime container itineraries for anti-fraud and supply chain security. In: EUROPEAN

INTELLIGENCE AND SECURITY INFORMATICS CONFERENCE, Odense. **Anais...** IEEE, 2012. p.76–83.

CHANDOLA, V.; BANERJEE, A.; KUMAR, V. Anomaly detection: a survey. **ACM Computing Surveys**, New York, v.41, n.3, p.1–58, jul. 2009. ACM.

CHAO, H.; GU, Y.; NAPOLITANO, M. A survey of optical flow techniques for robotics navigation applications. **Journal of Intelligent & Robotic Systems**, Greece, v.73, n.1-4, p.361–372, jan. 2014. Springer Science & Business Media.

CHAUDHRY, R. et al. Histograms of oriented optical flow and binet-cauchy kernels on nonlinear dynamical systems for the recognition of human actions. In: IEEE CONFERENCE ON COMPUTER VISION AND PATTERN RECOGNITION, Miami. **Anais...** IEEE, 2009. p.1932–1939.

CHEN, C. et al. iBOAT: isolation-based online anomalous trajectory detection. **IEEE Transactions on Intelligent Transportation Systems**, Los Angeles, v.14, n.2, p.806–818, jun. 2013. IEEE.

CHEN, S.; GANGOPADHYAY, A. A novel approach to uncover health care frauds through spectral analysis. In: IEEE INTERNATIONAL CONFERENCE ON HEALTHCARE INFORMATICS, Philadelphia. **Anais...** IEEE, 2013. p.499–504.

COLLINS, J. C. Using Excel and Benford's Law to Detect Fraud: learn the formulas, functions, and techniques that enable efficient benford analysis of data sets. **Journal of Accountancy**, Durham, v.223, n.4, p.44, apr. 2017. American Institute of CPA's.

CROUCHER, J. S. An upper bound on the value of the standard deviation. **Teaching Statistics**, Brisbane, v.26, n.2, p.54–55, may 2004. Wiley.

CUTLER, R.; TURK, M. View-based interpretation of real-time optical flow for gesture recognition. In: THIRD IEEE INTERNATIONAL CONFERENCE ON

AUTOMATIC FACE AND GESTURE RECOGNITION, Nara. **Anais...** IEEE, 1998. p.416–421.

DAI, Y. et al. Online Credit Card Fraud Detection: a hybrid framework with big data technologies. In: TRUSTCOM BIGDATASE ISPA, 2016 IEEE, Tiajin. **Anais...** IEEE, 2016. p.1644–1651.

DAVID, L. P.; ALAN, K. M. **Artificial Intelligence Foundations of Computational Agents**. 1.ed. Cambridge: Cambridge University Press, 2010.

DEONIER, R. C.; TAVARÉ, S.; WATERMAN, M. S. **Computational genome analysis**: an introduction. 1.ed. California: Springer Science & Business Media, 2005.

DONG, F.; SHATZ, S. M.; XU, H. Inference of online auction shills using dempster-shafer theory. In: SIXTH INTERNATIONAL CONFERENCE ON INFORMATION TECHNOLOGY: NEW GENERATIONS, Las Vegas. **Anais...** IEEE, 2009. p.908–914.

DOWNEY, A. B. **Think stats**. 2.ed. Sebastopol: O'Reilly Media, Inc., 2014.

EFRON, B.; TIBSHIRANI, R. J. **An introduction to the bootstrap**. 1.ed. Boca Raton: CRC Press, 1994.

FORMANN, A. K. The Newcomb-Benford law in its relation to some common distributions. **PloS One**, Tehran, v.5, n.5, p.1–13, may 2010. John Innes Centre.

GARCIA, S.; LUENGO, J.; SAEZ, J. A survey of discretization techniques: taxonomy and empirical analysis in supervised learning. **IEEE Transactions on Knowledge and Data Engineering**, Sydney, v.25, n.4, p.734–750, 2013. IEEE.

GEORGE, S. L.; BUYSE, M. Data fraud in clinical trials. **Clinical investigation**, Michigan, v.5, n.2, p.161–173, nov. 2015. NIH Public Access.

GHUSE, N.; PAWAR, P.; POTGANTWAR, A. An Improved Approch For Fraud Detection In Health Insurance Using Data Mining Techniques. **International Journal of Scientific Research in Network Security and Communication**, Sochi, v.5, n.3, p.27–33, jun. 2017.

GONZALEZ, R.; WOODS, R. **Digital image processing**. 2.ed. New Jersey: Prentice Hall, 2002.

HAAS, S. D.; WINKER, P. Detecting fraudulent interviewers by improved clustering methods–the case of falsifications of answers to parts of a questionnaire. **Journal of Official Statistics**, Warsaw, v.32, n.3, p.643–660, sep. 2016. De Gruiter.

HAN, J.; PEI, J.; KAMBER, M. **Data mining concepts and techniques**. 3.ed. Waltham: Elsevier, 2011.

HE, H.; TAN, Y. A two-stage genetic algorithm for automatic clustering. **Neurocomputing**, Middlesex, v.81, n.1, p.49–59, apr. 2012. Elsevier.

HEIN, J. et al. Scientific fraud in 20 falsified anesthesia papers. **Der Anaesthesist**, PauwelstraBe, v.61, n.6, p.543–549, jun. 2012. Springer.

HODGE, V. J.; AUSTIN, J. A survey of outlier detection methodologies. **Artificial intelligence review**, Chicago, v.22, n.2, p.85–126, oct. 2004. Springer.

HU, W. et al. A survey on visual surveillance of object motion and behaviors. **IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)**, Prague, v.34, n.3, p.334–352, aug. 2004. IEEE.

HUI, G. et al. On-road remote sensing measurements and fuel-based motor vehicle emission inventory in Hangzhou, China. **Atmospheric Environment**, Hong Kong, v.41, n.14, p.3095–3107, may 2007. Elsevier.

HÜLLEMANN, S.; SCHÜPFER, G.; MAUCH, J. Application of Benford's law: a valuable tool for detecting scientific papers with fabricated data? **Der Anaesthesist**, Heidelberg, v.66, n.10, p.795–802, oct. 2017. Springer.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA. Avaliação da Conformidade, 5ª Edição, Rio de Janeiro, 2007, Acesso: 15/12/2012, <http://www.inmetro.gov.br/inovacao/publicacoes/acpq.pdf>.

INSTITUTO NACIONAL DE METROLOGIA, QUALIDADE E TECNOLOGIA. Aplicação de Sanções aos Organismos de Avaliação da Conformidade, versão 3, Rio de Janeiro, 2017, Acesso: 30/12/2017, <http://www.inmetro.gov.br/Sidoq/pesquisa_link.asp?seq_tipo_documento=3&cod_uo_numeracao=00581&num_documento=141>.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION/INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 17000** - Vocabulary and general principles, Geneva, 2004.

JINKA, P.; RAO, G.; SUNDARARAMAN, K. ClaimPerfect: an application case study of machine learning techniques towards a fraud management system for warranty claims processing. In: INTERNATIONAL CONFERENCE ON UBIQUITOUS INFORMATION MANAGEMENT AND COMMUNICATION, 6., Kuala Lumpur. **Proceedings...** ACM, 2012.

JOUDAKI, H. et al. Using data mining to detect health care fraud and abuse: a review of literature. **Global journal of health science**, Toronto, v.7, n.1, p.194–202, jan. 2014. Canadian Center of Science and Education.

JOUDAKI, H. et al. Improving fraud and abuse detection in general physician claims: a data mining study. **International journal of health policy and management**, Kerman, v.5, n.3, p.165–172, mar. 2016. Kerman University of Medical Sciences.

KAY, R. U. Fundamentals of the Dempster-Shafer theory and its applications to system safety and reliability modelling. **Reliability and Theory Applications**, San Diego, v.2, n.3-4, p.173–185, dec. 2007.

KIM, I. S. et al. Intelligent visual surveillance - a survey. **International Journal of Control, Automation and Systems**, Chonbuk, v.8, n.5, p.926–939, oct. 2010. Springer.

KITCHENHAM, B. et al. Systematic literature reviews in software engineering â A systematic literature review. **Information and Software Technology**, Alberta, v.51, n.1, p.7–15, jan. 2009. Elsevier.

KOPRINSKA, I.; CARRATO, S. Temporal video segmentation: a survey. **Signal processing: Image communication**, Paris, v.16, n.5, p.477–500, jan. 2001. Elsevier.

KOSE, I.; GOKTURK, M.; KILIC, K. An interactive machine-learning-based electronic fraud and abuse detection system in healthcare insurance. **Applied Soft Computing**, Iizuka, v.36, p.283–299, nov. 2015. Elsevier.

KUNDU, A. et al. Blast-ssaha hybridization for credit card fraud detection. **IEEE Transactions on Dependable and secure Computing**, Indiana, v.6, n.4, p.309–315, oct.-dec. 2009. IEEE.

KUNDU, A.; SURAL, S.; MAJUMDAR, A. K. Two-stage credit card fraud detection using sequence alignment. In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS SECURITY, Berlin. **Anais...** Springer, 2006. p.260–275.

LAKSHMI, B.; RAGHUNANDHAN, G. A conceptual overview of data mining. In: NATIONAL CONFERENCE ON INNOVATIONS IN EMERGING TECHNOLOGY, Erode. **Anais...** IEEE, 2011.

LANTZ, B. **Machine learning with R**. 1.ed. Birmingham: Packt Publishing Ltd, 2013.

LIPTON, A. J.; FUJIYOSHI, H.; PATIL, R. S. Moving target classification and tracking from real-time video. In: FOURTH IEEE WORKSHOP ON APPLICATIONS OF COMPUTER VISION, New Jersey. **Anais...** IEEE, 1998. p.8–14.

LIU, S.; NI, L. M.; KRISHNAN, R. Fraud detection from taxis' driving behaviors. **IEEE Transactions on Vehicular Technology**, Florida, v.63, n.1, p.464–472, jan. 2014. IEEE.

LU, F.; BORITZ, J. E.; COVVEY, D. Adaptive fraud detection using Benford's law. In: CONFERENCE OF THE CANADIAN SOCIETY FOR COMPUTATIONAL STUDIES OF INTELLIGENCE, Quebec. **Anais...** Springer, 2006. p.347–358.

LUCAS, B. D. **Generalized image matching by the method of differences**. Pittsburgh: University Microfilms International, 1986.

MANDAL, R.; CHOUDHURY, N. Automatic Video surveillance for theft detection in ATM machines: an enhanced approach. In: COMPUTING FOR SUSTAINABLE GLOBAL DEVELOPMENT (INDIACOM), 2016 3RD INTERNATIONAL CONFERENCE ON, New Delhi. **Anais...** IEEE, 2016. p.2821–2826.

MARQUES, O. **Practical image and video processing using MATLAB**. 1.ed. New Jersey: John Wiley & Sons, 2011.

MCGHEE, S. **Pairwise alignment of metamorphic computer viruses**. San José: San José State University, 2007.

MILOSAVLJEVIĆ, B.; PEŠIĆ, R.; DAŠIĆ, P. Binary logistic regression modeling of idle CO emissions in order to estimate predictors influences in old vehicle park. **Mathematical Problems in Engineering**, London, v.2015, p.1–10, may 2015. Hindawi Publishing Corporation.

MONTGOMERY, D. C.; RUNGER, G. C. **Applied statistics and probability for engineers**. 5.ed. New Jersey: John Wiley & Sons, 2010.

NEEDLEMAN, S. B.; WUNSCH, C. D. A general method applicable to the search for similarities in the amino acid sequence of two proteins. **Journal of molecular biology**, La Jolla, v.48, n.3, p.443–453, mar. 1970. Elsevier.

NIGRINI, M. **Benford's Law Applications for Forensic Accounting, Auditing, and Fraud Detection**. 1st.ed. New Jersey: John Wiley & Sons, 2012.

OPPENHEIM, A. v.; SCHAFER, R.; STOCKHAM, T. Nonlinear filtering of multiplied and convolved signals. **IEEE transactions on audio and electroacoustics**, Athens, v.16, n.3, p.437–466, sep. 1968. IEEE.

PAL, N. R.; JAMES, C. B. On cluster validity for the fuzzy c-means model. **IEEE Transactions on Fuzzy Systems**, Nottingham, v.3, n.3, p.370–379, aug. 1995. IEEE.

PAOLO, G. **Applied data mining statistical methods for business and industry**. 1.ed. New York: Wiley, 2003.

PENG, H.; YOU, M. The Health Care Fraud Detection Using the Pharmacopoeia Spectrum Tree and Neural Network Analytic Contribution Hierarchy Process. In: TRUSTCOM BIGDATASE, Tianjin. **Anais...** IEEE, 2016. p.2006–2011.

POGUE, J. M. et al. Central statistical monitoring: detecting fraud in clinical trials. **Clinical Trials**, London, v.10, n.2, p.225–235, jan. 2013. SAGE.

POZUELO, D.; DÍAZ, V.; BOADA, M. Improving Vehicle Safety: a new methodology for vehicle steering system inspection by means of forces measure. **Advances in Mechanical Engineering**, London, v.6, p.1–10, jan. 2014. SAGE Publications.

QIAO, X.; XU, A. Statistical Regularity of Vehicle Front Wheel Sideslip and Its Modeling. In: ICLEM 2010 SLOGISTICS FOR SUSTAINED ECONOMIC DEVELOPMENT: INFRASTRUCTURE, INFORMATION, INTEGRATION, Chengdu. **Anais...** ASCE, 2010. p.1588–1592.

RADKE, R. J. et al. Image change detection algorithms: a systematic survey. **IEEE transactions on image processing**, Charlottesville, v.14, n.3, p.294–307, mar. 2005. IEEE.

RASHIDIAN, A.; JOUDAKI, H.; VIAN, T. No evidence of the effect of the interventions to combat health care fraud and abuse: a systematic review of literature. **PloS One**, Tehran, v.7, n.8, p.e41988, 2012.

SHAFER, G. et al. **A mathematical theory of evidence**. New Jersey: Princeton University Press, 1976. v.1.

SHANMUGAM, G.; LOW, R. M.; STAMP, M. Simple substitution distance and metamorphic detection. **Journal of Computer Virology and Hacking Techniques**, Laval, v.9, n.3, p.159–170, aug. 2013. Springer.

SIEGEL, S. **Nonparametric Statistics for the Behavioral Sciences**. 1.ed. Tokyo: McGraw-Hill, 1956.

SMITH, T. F.; WATERMAN, M. S. Identification of common molecular subsequences. **Journal of molecular biology**, La Jolla, v.147, n.1, p.195–197, mar. 1981. Elsevier.

SOUZA, R.; CARMO, L. F. R. C.; PIRMEZ, L. Detecção de Dados Suspeitos de Fraude em Organismos de Inspeção Acreditados. In: XIV SIMPÓSIO BRASILEIRO EM SEGURANÇA DA INFORMAÇÃO E DE SISTEMAS COMPUTACIONAIS, Belo Horizonte. **Anais...** SBC, 2014.

SOUZA, R.; CARMO, L.; PIRMEZ, L. A procedure to detect suspected patterns of fraudulent behavior in vehicle emissions tests performed by an accredited inspection body. **Accred Qual Assur**, Geel, v.21, n.5, p.323–333, oct. 2016. Springer.

SOUZA, R.; CARMO, L.; PIRMEZ, L. An enhanced bootstrap method to detect possible fraudulent behavior in testing facilities. **Accred Qual Assur**, Geel, v.22, n.1, p.21–27, feb. 2017. Springer.

SOUZA, R. et al. Redes de Kohonen para detecção de fraudes em inspeções na área de transporte de produtos perigosos. In: VII CONGRESSO BRASILEIRO DE METROLOGIA, Ouro Preto. **Anais...** SBM, 2013.

SUN, C. et al. A Hybrid Approach for Detecting Fraudulent Medical Insurance Claims. In: INTERNATIONAL CONFERENCE ON AUTONOMOUS AGENTS & MULTIAGENT SYSTEMS, 2016., Singapore. **Proceedings...** International Foundation for Autonomous Agents and Multiagent Systems, 2016. p.1287–1288.

TAYLOR, R.; MCENTEGART, D.; STILLMAN, E. Statistical techniques to detect fraud and other data irregularities in clinical questionnaire data. **Drug information journal**, Panama City Beach, v.36, n.1, p.115–125, jan. 2002. SAGE.

THORNTON, D. et al. Categorizing and Describing the Types of Fraud in Healthcare. In: PROCEDIA COMPUTER SCIENCE, Baltimore. **Anais...** Elsevier, 2015. v.64, p.713–720.

TOTH, D.; AACH, T.; METZLER, V. Illumination-invariant change detection. In: IEEE SOUTHWEST SYMPOSIUM IMAGE ANALYSIS AND INTERPRETATION, 4., Austin. **Anais...** IEEE, 2000. p.3–7.

TRINH, H. et al. Detecting human activities in retail surveillance using hierarchical finite state machine. In: INTERNATIONAL CONFERENCE ON ACOUSTICS, SPEECH AND SIGNAL PROCESSING, Prague. **Anais...** IEEE, 2011. p.1337–1340.

WANG, L.; HU, W.; TAN, T. Recent developments in human motion analysis. **Pattern recognition**, England, v.36, n.3, p.585–601, mar. 2003. Elsevier.

WANG, S. L. et al. The evaluation of trustworthiness to identify health insurance fraud in dentistry. **Artificial Intelligence in Medicine**, Vienna, v.75, p.40–50, jan. 2016. Elsevier.

WEI, L. et al. A distributed intelligent framework for electricity theft detection using benford's law and stackelberg game. In: RESILIENCE WEEK (RWS), 2017, Wilmington. **Anais...** IEEE, 2017. p.5–11.

WENZEL, T.; BRETT, C. S.; ROBERT, S. Some issues in the statistical analysis of vehicle emissions. **Statistical Analysis and Modeling of Automotive Emissions**, Washington, v.3, n.2, p.1–14, sep. 2001. BUREAU OF TRANSPORTATION STATISTICS.

WITTEN, I. H.; EIBE, F.; HALL, M. A. **Data mining practical machine learning tools and techniques**. 3.ed. Burlington: Morgan Kaufmann, 2011.

WONG, W.; STAMP, M. Hunting for metamorphic engines. **Journal in Computer Virology**, Laval, v.2, n.3, p.211–229, dec. 2006. Springer.

YILMAZ, A.; JAVED, O.; SHAH, M. Object tracking: a survey. **ACM Computing Surveys**, New York, v.38, n.4, p.13, dec. 2006. ACM.

YONG, G. et al. A taxi driving fraud detection system. In: INTERNATIONAL CONFERENCE ON DATA MINING, 11., Vancouver. **Anais...** IEEE, 2011.

ZHANG, Y.; BISHOP, G. A.; STEDMAN, D. H. Automobile emissions are statistically gamma distributed. **Environmental science & technology**, Berkeley, v.28, n.7, p.1370–1374, jul. 1994. ACS publications.

ZHIJUN, H.; CHUANGWEN, X. Average Clustering of Discrete Data Based on Probability and its Application to Expressway Toll Fraud Detection. In: WRI GLOBAL CONGRESS ON INTELLIGENT SYSTEMS, Xiamen. **Anais...** IEEE, 2009. p.404–407.

ZHUANG, W. et al. Ensemble Clustering for Internet Security Applications. **IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)**, Piscataway, v.42, n.6, p.1784–1796, nov. 2012. IEEE.

ZIEGEL, E. R. **Probability and Statistics for Engineering and the Sciences**. 2.ed. Abingdon: Taylor & Francis, 2012.