CHAPTER 10

COMPUTER SCIENCE

Doctoral Theses

01. AGRAWAL (Tripti)
Improved Pre- processing of Social Media Text for Sentiment Analysis.
Supervisor: Prof. Archana Singhal
Th 26160

Abstract

Social networks provide a global platform for its users to express their opinions freely on diverse topics. The presence of millions of active users results in the generation of the voluminous opinionated data. This generated data act as a treasure trove for business organizations to understand public sentiments towards their brand and services. However, the problem with this lucrative opinionated data is that it is unstructured due to the presence of various informal linguistic features such as acronyms, slangs, misspelled words, emojis, emoticons, idiomatic expressions, and so on. To extract meaningful information from this data, it is required to handle these linguistic features and transform it into a usable format. The handling of these linguistic features is challenging due to the varying writing patterns of netizens. These varying patterns cause inconsistency and noise in the voluminous data to a great extent. The data preprocessing is an underlying and fundamental step in sentiment analysis as it facilitates a better understanding of the data by transforming unstructured data into a usable format, and thus enhances the efficiency and accuracy of sentiment classification results. In the proposed approach, to analyze the potential of different social networks for target brand marketing, a comparative study of various social networks has been done. Based on this study, an improved pre-processing approach for three different social networks, namely, Twitter, Google+, and Facebook, has been suggested. In the proposed pre-processing approach, various linguistic features have been classified into sentiment bearing and non-sentiment bearing linguistic features. The sentiment bearing features have been handled with the help of compiled dictionaries and all other features have been replaced with specific keywords. A list of comprehensive dictionaries has been compiled to handle the varying writing xiii patterns of netizens so that the dictionary lookup task can be performed with a high success rate. Apart from comprehensive dictionaries, the distinctive features of the proposed preprocessing sequence are the handling of emojis and idiomatic expressions. Among all the linguistic features, emojis are the highest sentiment bearing linguistic features and thus, have been handled in detail. A separate procedure for the handling of emojis with multiple interpretations has also been suggested. Using this procedure, each emoji is replaced with its emotional content depending on the textual context. Apart from emojis, idiomatic expressions are also important to be handled as these are also frequently used by netizens on social media. The meaning of these expressions is entirely different from the literal meaning of their constituent words. Due to this, the handling of idiomatic expressions is not possible with the help of existing sentiment analysis approaches. Therefore, idiomatic expressions have been handled with the help of a newly compiled dictionary. A procedure has also been proposed for the replacement of idiomatic expressions with their description from the compiled dictionary. In the proposed approach, additional pre-processing steps such as handling of codemixed data, hashtag handling, removal of HTML tags, etc. along with different procedures for username replacement in Google+ and Facebook have also been suggested. Thus, the proposed pre-processing approach is a mix of comprehensive dictionaries and different procedures along with few additional pre-processing steps. The proposed approach also suggests that the implementation of pre-processing steps in an ordered sequence enhances the results of the overall data pre-processing. There exists a slight variation in the pre-processing sequences of different social networks due to data disparity among the networks. Thus, an ordered pre-processing sequence for each social network has also been suggested. Further, experiments have been carried out to compare the proposed system with the existing ones. Results show that the proposed system outsmarts the past approaches mainly due to the implementation of pre-processing steps in an ordered sequence and handling of emojis. In addition to the data pre-processing of different social networks, the proposed preprocessing approach has been used to enhance the efficiency of the language prediction model using FastText on unstructured multilingual datasets. As a part of data pre-processing, the proposed pre-processing sequence also suggests an improved approach for data annotation of unlabeled data using a sentiment lexicon called VADER.

Contents

1. Introduction and motivation 2. Analysis of various social networks for target brand marketing 3. Background and related work 4. Data collection and linguistic features handling 5. Data pre- processing of twitter, Google+ and Facebook 6. Ordered sequences for data pre-processing of social networks 7. Enhancing fast text accuracy for language identification of multilingual data on Facebook 8. An improved approach for annotation of social media data using VADER 9. Conclusion and future scope and Bibliography.

02. BANSAL (Ritu Singhal Nee)
Feedback – Based Combinatorial Double Auction Model for Resource Allocation.
Supervisor: Prof. Archana Singhle
Th 26155

Abstract

The present The affordable cloud computing infrastructure has a major impact in the IT community. Cloud infrastructure have been evolved as an economical mode of achieving high performance processing tasks, in versatile areas such as business, research, science and finance. Cloud computing consists of computing services delivered remotely to the customers via the internet. The importance of cloud computing “anytime anywhere” facilities can lead to usage of technological advancements that can significantly contribute to the growth of the IT sector. The baseline of a proposed approach is to analyze the contribution of cloud computing to the advent of the ease of learning and facilitating education in an economical way, with limited budget, without limitation of physical boundaries. An “E-Cloud” architecture has been proposed for a university system to improve education at colleges as well as university level in a cost-effective manner. The e-waste generation in the educational sector due to IT facilities, is becoming an environmental hazard as proper disposal at a small level is an expensive affair. The importance of cloud resource utilization plays an effective role in controlling the e-waste generation thereby relieving from botheration of e-resources management and

proper e-waste disposal for green and healthy environment. E-Cloud has been suggested as a solution for e-waste management for the educational institutions. Proposed work also focuses on the study of availability of cloud resources for learners in remote areas and students with special needs. The Android application “Lecture Hall” using cloud storage demonstrates how the emerging cloud computing technology can improve accessibility to educational resources by Students with Visual Disabilities (SVD). Cloud computing provides the infrastructure in the form of virtual machines with different configurations based on CPU, memory, storage, and bandwidth on pay per usage model. There are popular pricing schemes namely fixed pricing scheme, dynamic pricing scheme, and auction pricing scheme. In the competitive market, the fixed price model is not successful as there are ups and downs in the market. In the dynamic model, the pricing scheme is used according to demand and supply flow, as seen in air reservation, booking of taxis, buses, railway reservations, and in online shopping. This is a one-sided business, and a customer is just a passive entity. Auction is another pricing scheme that offers a good solution over dynamic pricing as both customers and providers can participate actively. In the proposed approach, a combinatorial double auction framework is suggested that provides a platform to all the providers and customers to participate in the auction with their preferences. In the proposed work, initially, CEDARA model is suggested for an efficient market-based economical, fair resource allocation double auction model that allows both customers and providers to participate. It provides fair allocation of resources by promoting truthful providers and satisfies the resource requirements of customers with a good profit margin. An important trait in the online market is malicious providers who want to outperform their peers in any situation, making everyone else lose a chance to sustain in the market. These market spoilers book losses in the beginning to make their identity. It demotivates the other providers to participate in auction, leading to reduced availability of resources. A second Model named as CFEDARA, is proposed that promotes truthful providers and penalizes market spoilers to promote fairness in the system. It simultaneously benefits users by satisfying their resource requirements within their budget. It has shown increased participation of providers and customers incorporating genuineness and truthfulness as compared to the existing approaches while maintaining the overall profit and resource utilization. In the current market scenario, the online market has emerged as one of the most expedient markets. When many companies become a part of the online market, feedback and price play an important role in their sustainability. A provider who is providing required resources at a very economical price may not provide the required quality of service as per the expectations of the customers. So, the customers’ feedback becomes an important criterion for the overall evaluation of the proposed system. A Feedback based Combinatorial Fair Economical Double Auction Resource Allocation Model (FCFEDARA) is suggested as an improved version of CEDARA and CFEDARA. This model promotes genuine providers with good feedback, discourages market spoilers, and promotes fairness in the system to enhance provider and customer trust level in the system. Three variants of the feedback-based approach have been analyzed with their strength and limitations. The proposed model is dynamic and evaluated under the CloudSim environment. The criteria include customer feedback, type, and number of resources, number of customers, number of providers, and bundle bids provided by providers and customers. It is evaluated on diverse permutations of providers and customers and analyzed diverse scenarios of the actual market. The results have shown significant improvement over existing models in maintaining fairness as well as trustworthiness. There is an increase in resource utilization due to the algorithmic approach to enhance the participation of more providers and customers. The proposed model successfully maintained the truthfulness by promoting genuine providers, quality of service for the premium customers as well as retained the demand and supply flow of the market.

Contents

1. Introduction and motivation 2. Application of cloud computing in education system 3. A combinatorial economical double auction resource allocation model (CEDARA) 4. A combinatorial fair economical double auction resource allocation model (CFEDARA) 5. A feedback- based combinatorial fair economical double auction resource allocation model 6. Analysis of case 2 and case 3 of FCFEDARA model for winner 7. Conclusion and future work. Appendix A supplementary material and References.

03. CHOPRA (Akanksha Bansal)
Detection of Push and Nuke Attacks in Recommender Systems.
Supervisor: Dr. V.S. Dixit
Th 26156

Abstract

E- Commerce industry has taken an edge over Internet in the past few decades. Customers surf e-commerce websites to select the target product. Some of the popular e-commerce websites such as amazon.com, flipkart.com, snapdeal.com etc., use a personalized decision making tool, called as Recommender System. Recommender System recommends the product to its users (or customers) on the basis of user data and product data. These systems can be categorized as Collaborative Filtering Recommender system, Content Based Recommender system and Hybrid Recommender system. Collaborative Filtering Recommender System makes recommendation based on similar user concept. The primary focus is given to user data by these systems. On the other hand, content based recommender systems focus on product features and make recommendations for the product. The Hybrid Recommender Systems, as the name suggests, makes use of both user data and product data to make recommendations. Out of these three, Collaborative Filtering Recommender System is the most popular and widely used approach by the e-commerce websites. Collaborative Filtering Recommender System makes recommendations based on user ratings that are given for the product. Based on these ratings and user data, similar users are clustered and recommendations are generated. The interested users take help of these recommendations to choose the target product. Additionally, these ratings are used to promote or demote the target product. The product with a maximum number of higher ratings is recommended by the system. Obviously, this product attracts the users and users intend to purchase such product. This increases the sales of such a highly rated product. With the open nature of Collaborative Filtering Recommender System, it is often, that factitious users intrude into the system and rate the target product. These factitious users may be the attackers or malicious users. Normally, they are the paid professionals who inject biased ratings for the target product to alter the recommendation list. The purpose behind injecting the attacks is to either promote the target product, thereby increasing its sales, or to demote the target product from the competitor company to decrease its sales. The higher biased rating is called Push Attack and the lower biased rating is called Nuke Attack. With the increasing demand of online products, the Collaborative Filtering Recommender Systems are bound to provide accurate and correct recommendations to its users. The primary goal of this research is to design a novel solution to detect these attacks that are injected by factitious users into Collaborative Filtering Recommender System. The reviews and ratings given by the users for a product are the key parameters to detect the attacks. The pre – processing is applied on the

user reviews and a Bag of Words is created. The features are extracted using the Term Frequency – Inverse Domain Frequency and Word2Vec methods. By applying Opinion Mining measures on the user reviews the attacks are detected. The designed model is named as Opinion Mining Polarity Subjectivity Model. This model limits itself in the situation where human sarcasm is involved. Thus, the research further designs a Hybrid Deep Neural Network Model using a hybrid approach to overcome the problems of human sarcasm. Hybrid Deep Neural Network model is designed by integrating Opinion Mining, Deep Neural Network and Harris Hawk Optimization Algorithm. The proposed model is applied on the user reviews that are given for the target product. The model consists of three main components – Input layer, Hidden layers and Output layer. Each layer has the associated nodes. Initially, the weights are assigned randomly to these nodes. The weights are then updated by Harris Hawks Optimization Algorithm. The dataset is split into the train set and the test set. The biased ratings are labeled as 'PUSH ATTACK', 'NUKE ATTACK' and genuine ratings are labeled as 'NORMAL' in the train set. By using the train set, the test set predicts the attacks. This model is designed for Collaborative Filtering Recommender System. The research work further extends for Hybrid Recommender System. Another model, named as Adaptive Recurrent Neural Network, is designed by integrating Opinion Mining, Recurrent Neural Network and Bald Eagle search Optimization Algorithm. The proposed model is applied on both user data and product data. The weights associated with the nodes in this model are initialized and updated by using Bald Eagle Search Optimization Algorithm. The train set is labeled and test set is used to predict the attacks. To enhance the recommendation quality, the proposed models use clustering techniques to group the similar users. The clustering techniques used in this research are Kmeans and Modified Density Peak Clustering Algorithm. The similarity between the users is computed using the similarity measures - Pearson Correlation Coefficient, Cosine Similarity Coefficient and Dice Similarity Coefficient. Further the proposed models are compared with the existing models. The performance measures used for comparison are Accuracy, Recall, Precision and F-measure. The results show that the proposed models outperform the existing models. The comparison between the proposed- Opinion Mining Subjectivity Polarity Model, Hybrid Deep Neural Network Model and Adaptive Recurrent Neural Network Model is also shown in the research. The results show that the proposed Adaptive Recurrent Neural Network Model is better than the other two proposed models and existing models. Therefore, this research tackles the attacks in Recommender Systems. The proposed models demonstrate the new techniques of integrating deep learning approaches with opinion mining approach and optimization algorithms. The proposed models are implemented on variety of datasets. This is because; any designed model must be flexible to be implemented on any type of dataset, as every dataset has its own features. To conclude, depending upon the nature of dataset, out of the proposed models, the best suited model can be chosen and applied to detect the attacks. The application of this work done in the e-commerce industry would yield good quality recommendations for the target product. This in turn, would benefit the users to select the correct product from the available online pool of products. The companies would be able to study the market trend more precisely, which is a key factor for their growth.

Contents

1. Introduction 2. Background 3.Need of detection of push and nuke attacks in CFRS 4. Opinion mining polarity subjectivity model 5. Hybrid deep neural network model 6. Adaptive recurrent neural network model 7. Conclusion and future work. References and List of publications.

04. DUARI (Swagata)

Complex Networks for Textual Discourse Coherence Analysis.

Supervisor: Prof. Vasudha Bhatnagar

Th 26161

Abstract

This thesis presents a study on computational discourse analysis of written communication. Discourse analysis deals with deciphering the meaning of communication in terms of two fundamental characteristics of a discourse: coherence and cohesion. Coherence is a cognitive property that asserts how well the text is making sense to the reader. Cohesion is a semantic property that expresses the continuity between one part of the text and another. Computational methods for modelling and analyzing these characteristics of a discourse attract immense interest from the computational linguistics research community. The work presented in this thesis exploits a complex network based framework for document representation to analyze the discourse coherence and cohesion of text documents. The proposed framework represents text as a complex network and analyzes the propensity of topological features to uncover hidden patterns and relationships. This research aims to model discourse characteristics of scientific, scholarly documents by scrutinizing the interplay of key-entities (keywords) in the text. In this regard, the main contributions of this thesis are - (i) developing two unsupervised, parameterless methods for automatic keyword extraction (sCAKE and LAKE) and a supervised, complex network-based keyword extractor (CnAKE),(ii) a fast-and-frugal coherence detection method (FFCD), (iii) a multilayer complex network-based representation of scholarly documents to capture the relationship among key-entities to assess cohesion, and (iv) an analytical framework, CHeck It Again Author (CHIAA), for quantitative and qualitative assessment of textual discourse.

Contents

1. Introduction 2. Background and preliminaries 3. Unsupervised keyword extraction 4. Language agnostic keyword extraction 5. Supervised keyword extraction 6. Discourse coherence analysis 7. Discourse cohesion analysis 8. Conclusion and future directions. A Indian language documents used in chapters 4 and 5 B Example of weakly coherent text block.

05. GUPTA (Neha)

Explainable Online Intrusions Detection System Handling Class Imbalance Problem.

Supervisors: Prof. Punam Bedi Dr. Vinita Jindal

Th 26150

Abstract

In recent times, the usage of the Internet has increased and consequently, the number of cyber intrusions targeting computer networks has also increased. These intrusions cause severe damage to the confidentiality, integrity, and availability of both data and devices connected over the Internet. To secure computer systems and networks against cyber intrusions, Intrusion Detection Systems (IDSs) are deployed in the real world. An IDS monitors the activities of a computer system/network and analyses those activities to detect intrusions. When an intrusion is detected by the IDS, it informs the administrator. Then, the administrator takes corrective measures for handling that intrusion. An IDS that secures a single computer system is known as a Host-based IDS (H-IDS) whereas an IDS that secures all the communications over a network is known as a Network-based IDS (N-IDS). Since most of the intrusions are performed through malicious communications between networked devices, this thesis focuses on developing a Network-based IDS for identifying such intrusions. Though many N-IDSs have been developed in the past, there still exist some major challenges in performing effective intrusion detection. The Class Imbalance problem is one of the major challenges that affect the performance of N-IDSs. The Class Imbalance problem arises when a dataset has an uneven distribution of samples in its classes. Such datasets are known as imbalanced datasets. In an imbalanced dataset, the class having a large number of samples is called the majority class and the class having a limited number of samples is known as the minority class. Due to the lack of samples, the classification of minority classes becomes difficult and this is known as the Class Imbalance problem. Network traffic classification is an example of an imbalanced classification problem. In computer networks, the amount of traffic present for infrequent intrusions is very less as compared to the amount of traffic available for frequently occurring intrusions and normal data. Since there exist a limited number of training samples for infrequent intrusions, it becomes difficult for N-IDSs to classify these intrusions correctly. Themisclassified intrusions can severely damage the security of a network. Therefore, an N-IDS must handle the Class Imbalance problem to ensure the complete security of the network. Furthermore, N-IDSs should also mitigate undetected intrusions (False Negatives) that are generated when intrusions get misclassified as normal traffic. In addition, timely detection of intrusions also plays a crucial role in securing any computer network. It allows the network administrator to respond to intrusions quickly and limit the damage caused by them. Moreover, an IDS should also mitigate false alarms (False Positives) which are generated when normal traffic gets misclassified as intrusive. False Positives burden the administrators by consuming their time and resources. Another challenge in intrusion detection is the inability of an IDS to process online network traffic. Most of the IDSs developed in the literature have been trained and tested on benchmark datasets only. These IDSs cannot automatically transform online network traffic into the features that were utilized during training. So, they require an additional module for automatic feature extraction to perform online intrusion detection. Moreover, there is a need to develop IDSs that can explain the reason for their predictions. This makes the intrusion detection process transparent and enhances the trust of stakeholders in the predictions made by the IDS. This thesis aims to develop an effective N-IDS that handles the above-mentioned challenges existing in IDSs. To handle the Class Imbalance problem of network traffic, Siam-IDS has been proposed in this thesis. Siam-IDS uses the Siamese Neural Network to compute the similarity between a pair of traffic samples and classifies them either into normal class or one of the attack classes. Siamese Neural Network utilizes two identical Deep Neural Networks (DNNs) which compute the feature representations of traffic samples to find the similarity between them using the Euclidean distance function. Siam-IDS identifies a larger number of minority attacks as compared to its counterparts, thereby successfully handling the Class Imbalance problem.

Contents

1. Introduction 2. Background and related work 3. Handling class imbalance problem using Siamese neural network 4. Mitigating false negatives using DNN, Siamese neural network and XGBoost 5 . Reducing the detection time using LSTM and I-OVO technique 6. Mitigating false positives using cost-sensitive DNN, bagging and boosting ensembles. 7. Explainable cost-sensitive IDS using online network traffic features 8. Conclusion and direction for future work. References and Appendix.

06. SINGH (Prerna)
Diagnosis of Dental Caries Using Machine Intelligence.
Supervisor: Prof. Priti Sehgal
Th 26153

Abstract

Dental caries is defined as the oral disease which is caused by the bacteria “Mutans streptococci”. This bacterium is present in sugar and carbohydrates in food and drinks. The bacteria affect the tooth which results in pain and loss of tooth. A poor oral health and eating a diet rich in carbohydrates results in dental caries. People of all ages from childhood to senior years can get tooth decay or dental caries. The early diagnosis of dental caries is very important for the effective and timely treatment. The diagnosis of the dental caries is done by the dentist by analyzing a dental X-ray or radiograph. The dental radiograph gives a clear picture of the dental health. The dental X-rays can be taken of different views of the mouth. The different views are required depending on the number of teeth impacted by the caries. There are three types of dental X-rays showing different views of the mouth, namely, bitewing, periapical and panoramic. These dental X-rays captured by the X-ray machine can be converted into digital images and stored in computer system for further processing. These images can be enhanced further to investigate the problem areas. The present work is an attempt to use machine intelligence to diagnose dental caries. Segmentation plays an important role in identifying the actual objects that need to be classified in the targeted problem. Hence, an exhaustive survey of the various segmentation techniques on the three types of dental images i.e., the panoramic, the periapical and bitewing has been carried out in the beginning of this research work. The performance analysis of this survey helps to investigate which segmentation technique under various categories such as Edge Detection, Thresholding, Deformable Model and Clustering, is best suited for dental images.

Contents

1. Introduction 2. Theoretical basis 3. Dental image segmentation, numbering and classification of dental images 4. Caries detection and classification of digital dental X-ray images 5. G.V. Black classification of the dental images 6. Classification of dental caries based on the severity 7. Conclusion and future work. Bibliography. Appendix I and List of publications.

07. SINGHAL (Anuradha)
Universal Image Steganalysis Using Deep Learning Techniques.
Supervisor: Prof. Punam Devi
Th 26152

Abstract

Data transmission over the Web has increased multifold these days with more and more people using the internet. This gives an opportunity to fraudulent players for secret communication over the Web. Camouflaged communication using a media is known as Steganography. Steganography provides a secret way to carry out transmission in any form of medium such as text, image, audio, video, or network packets. Steganalysis tries to detect and find details of such secret communication. Hidden messages, also termed as payload may be encrypted before hiding in a cover object. These days, lot of information is transmitted over the internet and in social media in the form of digital images making them a viable form of media for carrying covert communication. Detection of concealed exchange or unraveling the details of such transmission in images is known as Image Steganalysis. Image Steganalysis can be broadly classified as active and passive steganalysis. Passive steganalysis can be binary or multi-class steganalysis. Binary steganalysis identifies an image as either stego or clean, whereas multi-class steganalysis can classify the images in multiple classes on the basis of used embedding algorithm. With the increase in counterfeit exchange over the internet via web pages, unravelling various details like hidden message length and region along with stego key details can be helpful to mitigate malicious exchange. Finding these details form a part of active image steganalysis. Active steganalysis is also termed as forensic steganalysis. Universal image steganalysis detects or unveils details about hidden messages in images of both spatial and JPEG domain without any knowledge about used steganography algorithm. Very few research papers are present in literature on active image steganalysis to the best of our knowledge. Majority of techniques present in image steganalysis literature are passive in nature with less emphasis on unveiling details of hidden message. Further, most of the techniques present in literature on active image steganalysis are not universal. They work in either spatial or JPEG domains. Moreover, stego images generated with individual embedding algorithms were used for training and testing the models in literature without mixing stego images generated from various embedding algorithms. Image Steganalysis techniques presented in this thesis are universal which work in both spatial and JPEG domains and are also not restricted to a steganographic algorithm. Various Deep Learning (DL) methods have been used for steganalysis in this work. Experiments have been performed in Keras python library 3.6 on gray scale images from standard BOSSBase dataset. Convolutional Neural Network (CNN) is one of the best known architectures used for image steganalysis. Problem of vanishing/exploding gradient arises as the depth of CNN increases. Residual Networks are used to solve the problem of the vanishing/exploding gradient in deep CNN. Residual Networks use skip connections by skipping training of few layers. Multi-class universal image steganalysis framework using Deep Residual Network (DRN) has been proposed for classifying stego images according to the used embedding algorithm. Confusion matrix, accuracy, precision and recall have been used as performance metrics. Obtained results are comparable with state-of-the-art techniques present in literature. After identification of embedding algorithm, frameworks for payload length estimation and region detection are proposed.

Contents

1. Introduction 2. Background and related work 3. Multi-class universal image steganalysis using deep residual network 4. Universal quantitative image steganalysis using CNN with LSTM 5. Universal quantitative image steganalysis using pre-trained ResNet-50 6. USteg-DSE: Universal quantitative image steganalysis using DenseNet merged with squeeze-and-excitation block 7. Estimating cover image for universal payload region detection in stego images 8. Conclusion and directions for future work. References and Appendies.

08. TANEJA (Sheetal Rajpal nee Seetal)
Use of Explainable Al in Biomarker Discovery for Breast Cancer Stratification and Interpretation of Proposed COVID-19 Detection Models.
Supervisors: Prof. Naveen Kumar and Dr. Manoj Agarwal
Th 26154

Abstract

Machine learning has been extensively used for constructing models that identify useful patterns from data and output decisions/ predictions with minimum human intervention. However, the models so constructed have traditionally operated like

black boxes and do not indicate the rationale behind their decisions to the end-user. Fortunately, in recent years, several model-specific and model-agnostic explainable AI methods have been developed that aid in interpreting the outcome of the machine learning models. These methods attempt to answer why a model is making a given prediction and when to trust a model. Answers to such questions assist in understanding the model's behavior. In this thesis, we have applied explainable AI methods to (i) discover relevant biomarkers that play a pivotal role in breast cancer stratification, and (ii) locate the affected lung regions in the case of COVID-19 patients. Breast cancer is a leading cause of cancer-related deaths among women. Availability of multi-omic data in recent years has revolutionized the methodology to unravel molecular mechanisms underlying the heterogeneity in breast cancer subtypes, namely, Basal, Her2, LumA, LumB, and Normal-like. Discovery of a minimal set of biomarkers that would enable the stratification of breast cancer plays an important role in devising therapeutic plans for the patients. Existing biomarker discovery algorithms for breast cancer stratification typically yield a set of biomarkers--- often too large to be interpreted clinically. In this thesis, we have exploited the power of explainable AI methods for the discovery of small sets of biomarkers based on gene expression, variations in copy number, and the extent of methylation for dissecting the heterogeneity of breast cancer. Towards this end, we have developed a deep learning framework for breast cancer stratification and analyzed it using different explainable AI methods. Thus, we have been able to identify small sets of biomarkers that achieve higher accuracy than what has been reported in recent works. Further, the discovered biomarkers have revealed statistically significant pathways known to be linked with different breast cancer subtypes. Survival analysis has revealed that the majority of biomarkers are prognostically relevant. Using the Drug Gene Interaction Database (DGIdb), we find that many of these discovered biomarkers are potentially druggable. Finally, validation on an independent cohort has established the efficacy of the identified biomarkers in breast cancer stratification. Severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) is a strain of coronavirus that causes the respiratory disorder-coronavirus disease 2019 (COVID-19). The reverse transcription-polymerase chain reaction (RT-PCR) test, considered to be a gold standard for COVID-19, suffers from a high false-negative rate. As an alternative, machine learning techniques are being intensely pursued for detecting COVID-19 using chest X-ray images. However, the challenge lies is separating COVID-19 cases from pneumonia as pneumonia affects the lungs in a manner similar to COVID-19. In this work, we have modeled the problem of detecting COVID-19 as a multiclass classification problem involving thre classes, namely, normal, COVID-19, and pneumonia. Towards this objective, we have proposed two classification models: the first model is an Extreme Learning Machine (ELM) that exploits its relatively short training time, and the second model is a hybrid model that exploits a set of features based on domain knowledge in conjunction with another set of features obtained using the ResNet-50 framework. The proposed models not only achieve good classification accuracy but using explainable AI methods, they also enable us to localize the affected regions. The regions, thus localized, have been verified by a radiologist. In summary, the use of explainable AI methods has provided insightful reasoning about the behavior of the deployed computational models by uncovering the contribution of the input features, leading to the selection of biomarkers for breast cancer stratification and localization of lung regions affected by COVID-19.

Contents

1. Introduction 2. Background 3. Biomarker discovery for breast cancer stratification using RNA sequence data 4. Biomarker discovery for breast cancer stratification copy number variation data 5. Biomarker discovery for breast cancer stratification using methylation level data 6. An extreme learning machine based model for COVID-19 detection and its interpretation 7. ResNet-50 based deep learning model for COVID-19 detection and its interpretation 8. Conclusion and scope of future work. Bibliography.

09. VERMA (Anjani Kumar)
Handling Profile Injection Attacks in Collaborative Filtering Based Recommender Systems.
Supervisor: Dr. V.S. Dixit
Th 26151

Abstract

The rapid expansion of the World Wide Web (WWW) and e-commerce has led to a serious problem of information overload; it leads to stress on surfers as they lose time on web surfing. They are not able to choose the right product without wasting too much time. From a large collection of items, Web Recommender Systems (RSs) help the users or surfers find the items that are going to be of interest to them from a large collection of items. In simple terms, RS makes it easier to handle the problem of information overload on the web by creating customized recommendations for users. RS helps users to make quality decisions and, in turn, find the items they would like to favor the most. There are three major types of RS, which work primarily in the area of e-commerce, namely: Collaborative Filtering (CF), Content-Based Filtering (CBF), and Hybrid Recommender Systems. The collaborative filtering approach assumes that human preferences are correlated, which means like-minded users will rate things similarly. Thus, explicit ratings are the typical input of this approach. The Content-Based Filtering approach recommends items based on items with similar properties to those that a user liked before, which can be seen in In a hybrid recommender system, it extracts the best of every recommendation technique to optimize the recommendations. These types of recommenders integrate multiple approaches to improve recommendation performance. As per the studies, two things were observed. First, when an attacker uses a genuine user profile to give ratings in a specific manner, it becomes hard to identify whether an attacker has injected the rating or a genuine user in a recommendation system. These are known as Profile Injection Attacks (also known as Shilling Attacks). This is further categorized into Push attacks, which are used to promote the system, and Nuke attacks, which are used to demote the system. Second, the profiling attack by someone affects the performance of the RS, which means it misleads the information, which is different from the actual rating. It also harms the data of online e-commerce applications by increasing their popularity. To overcome the problem, handling the shilling profiles becomes imperative. This research aims to explore approaches for recommending items that use the explicit behavior of users. Rating data is one such form of explicit data in which the user's navigational and behavioral parameters are traced to recommend the most suitable items. Preprocessing is applied to the data to obtain explicit details about a user, like rating and viewing an item. After justifying the valuable predictors, the next step is to predict the ratings on the navigational behavior of users. A framework has been developed to deploy the techniques and generate the recommendations and prevent profile injection attacks. By keeping these two points in mind, in this thesis, a recommendation framework using a Collaborative Filtering (CF) approach with

PIA models is proposed, which not only aims to generate secure recommendations but also to overcome the problem of profile injection attacks. Here, we have focused on the average attack in the push model and the love-hate attack in the nuke model. Therefore, this research tackles the attacks on recommender systems. The proposed models demonstrate the new techniques of integrating deep learning with the clustering approach and optimization algorithms. The proposed models are implemented on a variety of datasets. This is because any designed model must be flexible enough to be implemented on any type of dataset, as every dataset has its own features. To conclude, depending upon the nature of the dataset, out of the proposed models, the best-suited model can be chosen and applied to detect the profile injection attacks. The application of this work in e-commerce applications would yield good quality recommendations for the target item. This, in turn, would benefit the users by allowing them to select the correct item from the available pool of items online. Hence, the secure recommendations will help to enhance the popularity of the recommender system.

Contents

1. Introduction 2. Background 3. Complete overview of proposed framework 4. Profile injection attacks detection using classification and clustering based approaches 5. Hybrid framework for profile injection attacks detection 6. Prevention from profile injection attacks using secret credential method 7. Prevention from profile injection attacks using facial recognition 8. Conclusion and future work. List of publications and References.