CHAPTER 12

COMPUTER SCIENCE

Doctoral Theses

01. ARORA (Nidhi) nee Nidhi Bhatia
Enhancing Group Search Optimization Algorithm for Structural Analysis of Small Scale Networks
Supervisor : Dr. Hema Banati
Th 23969

Abstract
(Verified)

Complex interconnections among real world entities can be modelled in the form of networks, to gain a deeper insight into their structural and behavioural properties, often called as *Structural Network Analysis* (SNA). Extraction of densely connected communities (Community Detection (CD)) and influential nodes (Influence Maximization (IM)) are two main complex analytical problems in this domain. The work presented in this thesis aims at developing efficient solution methodologies for these two problems by enhancing a NI Group Search Optimization (GSO) algorithm. Some novel enhancements to basic GSO algorithm are presented in this thesis, which aim at customizing GSO algorithm for efficiently solving CD and IM problems in a novel manner. For CD problem, the developed solution methodologies are: a Modified '*Mod-GSO*' (Modified GSO); a node similarity enhanced '*E-GSO'* (Enhanced GSO); a hybrid '*TL-GSO'* (Teacher Learner- GSO)'; a discrete hybrid *'DTL-GSO'* (Discrete TL-GSO) and a Multi objective *'MGSO'*. These solution methodologies present novel ideologies to enhance a chosen NI algorithm for its wider applicability. Operationalizing identified communities in practical scenarios by identification of community specific leader nodes is one of the extended roles of network analytics. The thesis presents a novel "*node_rank*" metric to identify such community specific significant nodes to act as leaders. For IM problem, the developed solution methodologies are: '*IM-GSO*' (Influence Maximization using GSO) and *'IIM-GSO'* (Improved IM-GSO). IM-GSO and IIM-GSO smartly exploits hidden structural patterns of a network; like clusters, node degrees, betweenness and node similarities following a modular approach. The developed GSO based solution methodologies for improving *Structural Network Analysis* have shown significantly better results as compared to many heuristic/meta-heuristic based solution methodologies. With practical applications in many real life spheres, the presented solution methodologies can be very efficient in handling complex problems with higher accuracy.

Contents

1. Introduction 2. Structural network analysis 3. Group search optimazation for community detection 4. Variation of MOD-GSO algorithm 5. Identifying leaders from communities 6. Group search optimization for influenace maximization 7. Conclusion.

02. DABAS (Neelam)
Watermarking using Extreme Learning Machine
Supervisor : Dr. Ram Pal Singh
Th 23968

Abstract
(Not Verified)

The human society is fast transforming into a knowledge centric ecosystem catering to the production, dissemination and control of information and data. Digital data security can be provided by digital image watermarking. The objective of this study is to develop more robust, imperceptible and fast watermarking schemes. Three approaches have been proposed in this study by using computationally intelligent techniques called extreme learning machine (ELM) and its variants namely online sequential extreme learning machine (OSELM), weighted extreme learning machine (WELM), kernel extreme learning machine (KELM) and reduced kernel extreme learning machine (RKELM). The first proposed approach is simulated using ELM, OSELM and WELM in discrete wavelet transform (DWT) domain for colored images. Embedding of watermark is done in the LL sub-band of the two-level DWT domain by using the trained machine. The machine is trained by using the data-set which contains the relationship between neighboring pixels. The same trained machine is used to extract the watermark. In the second proposed approach, watermarking is implemented with singular value decomposition (SVD) in the integer wavelet transform (IWT) domain by using ELM and OSELM. Watermark is embedded in the LL sub-band of the one-level IWT domain by modifying the singular values of each block. Extraction of watermark is done by using the trained machine. The third approach is proposed by using KELM and RKELM. The watermark is embedded in the HL sub-band of one-level IWT domain by using the Cox's formula and extraction is done by using the trained machine. The proposed watermarking schemes outperform contemporary watermarking methods based on other machine learning techniques and are more robust and have efficient performance parameters. Further the proposed watermarking schemes based on OSELM and RKELM are found to have utility in real time applications because of high speed and lesser computational complexity.

Contents

1. Introduction 2. Literature survey 3. ELM and OSELM based watermarking scheme in DWT domain 4. SVD-IWT based watermarking scheme with ELM and OSELM 5. ELM-Kernel and reduced kernael ELM based watermarking scheme 6. Conclusion. References.

03.   RAJPAL (Ankit)
Watermarking Scheme for Images and Videos using Extreme Learning Machine and its Variants
Supervisors : Dr. Rajni and Dr. Anurag Mishra
Th 23970

Abstract
(Verified)

The circulation of digital multimedia content on the Internet often fall preys to the undesirable and often illegal operations such as duplication, modification, forgery, and copyright infringement. Therefore, the digital watermarking techniques have been developed for copyright protection, content authentication, and ownership identification of multimedia content such as image and video. Real time applications like video streaming necessitate that the time span of the watermarking process is minimized. However, this issue has not received enough attention in the literature. Extreme learning machine (ELM) being a faster alternative to back-propagation networks (BPNs) that are inherently slow and get stuck in the local minima, we have exploited the efficiency of the ELM and its variants such as online sequential ELM (OS-ELM) and bidirectional ELM (B-ELM) to develop time-efficient, visually imperceptible, and robust watermarking schemes. We began by proposing ELM based semi-blind watermarking schemes in the DWT domain for grayscale and color images. We then

developed OS-ELM based blind watermarking schemes using single as well as multiple scaling factors and found that the scheme using multiple scaling factor scores over the scheme based on the single scaling factor. Motivated by the computation of time efficiency of B-ELM in other applications, we developed B-ELM based watermarking schemes and found the resulting scheme is faster as compared to the watermarking schemes developed earlier. Finally, we developed a watermarking scheme for the compressed MPEG-4 videos using B-ELM that makes use of a novel fuzzy inference system based method for frame identification and selection. In all cases, we found that the proposed watermarking schemes score over their competitors in terms of visual quality and robustness against image processing attacks. Further, as the proposed algorithms consume only millisecond time span, these are suitable for developing real-time image and video processing applications

Contents

04. RICHA
Cross Doman Context : Aware Recommender System using Trust and Distrust
Supervisor : Prof. Punam Bedi
Th 23971

Abstract
(Not Verified)

Ease of availability of information with the rapid growth of internet results in the information overload problem for the user. Recommender Systems (RSs) help the users to handle information overload by making the process of search and selection easy, assisting them identify the items of their interest. This work presents a Cross Domain Context-aware Recommender system using Trust and Distrust (TDCDCARS) in a multi-agent environment to improve the quality of recommendations and to enhance the user acceptance. This system is proactive in nature and incorporates the user's contextual information at the time of recommendation generation. Recommendations are given by the system to the users at the right time without explicit request from the user. Cross domain recommender system is proposed and developed to reduce the sparse data problem. The developed system also uses the concept of distrust along with trust and reputation to safeguard the systems from the malicious users. To accelerate the computations, the system is parallelized using General Purpose Graphical Processing Unit (GPGPU), Compute Unified Device Architecture (CUDA) and Java for CUDA (JCuda). During the decision- making process, it is important to consider the social aspect i.e. trust and reputation at the time of computation. In the real world, we come across with the people whose opinions are helpful and also the people whose opinions cannot be trusted. This leads to another important aspect in this area, 'distrust', which is equally important to trust. TDCDCARS is a network of agents in which agents interact with each other in order to accomplish a goal. The architecture of the system is divided into five phases namely i) preprocessing phase, ii) cross domain similarity computation phase, iii) trust computation phase, iv) distrust computation phase, and v) prediction computation and selection of top-N recommendation.

Contents

1. Introduction 2. Basic concepts 3. Trust and reputation based collaborative filtering (TRbCF) 4. Proactive context aware recommender system (PCARS) 5. Proactive cross domain context aware recommender system 6. Proactive cross domain context aware recommender system using trust and distrust (TDCDCARS) 7. Conclusion and future work. References.

05.   SHARMA (Chhavi)
Community Detection Based Recommender Systems
Supervisor : Prof. Punam Bedi
Th 23967

Abstract
(Not Verified)

In this thesis, we have proposed techniques to handle some of the shortcomings and challenges in Recommender Systems research. Cold start problem is one of them. When a new user or an item enters the system, the information about user choices is insufficient to generate recommendations. The social network graph of the user can help to identify communication patterns and relationships of users which may be effective to delve into their tastes and analyse their choices. In this work, the social network (Facebook) data of the user has been utilised to overcome user cold start problem and generate book recommendations. Popularity bias is a phenomenon which leads to certain popular and most opted items to be repeatedly picked for recommendation. Modified Collaborative Filtering for Novel Recommendations (MCFNR) algorithm has been proposed in this thesis to handle popularity bias using Novelty Score metric. The concept of novelty has also been applied to the data extracted from Online Social Network (OSN) - Twitter in order to generate novel hashtag recommendations. A framework for Community based Collaborative Filtering Recommender System (CCFRS) is proposed in this work by combining community detection with CF technique. Louvain method is used for detecting the communities in a network. A prototype of the system has been developed and experiments have been conducted using the movie lens and book crossing dataset. Further, a framework for Community based Hashtag Recommender System (CHRS) is proposed and tested using a dataset collected via tweet pooling. Community based RS is combined with cross domain approach to propose – Community Detection based Cross Domain Recommender System (CCDRS). This system generates community detection based recommendations and uses the source domain to handle new item problem of the target domain. The system has been developed and tested for movies and books dataset.

Contents

1. Introduction 2. Basic Concepts 3. Handling cold start problem using interaction based social 4. Mitigating popularity bias in recommender systems using novelty score 5. Recommender systems based on community detection 6. Community detection based cross domain recommender systems 7. Conclusion and future work .References.

06.   VERMA (Sushma)
Techniques for Enhancing the Security of Android Framework.
Supervisor : Prof. Sunil Kumar Muttoo
Th 23972

Abstract
(Verified)

Android is an extensively used mobile platform leading the consumer market of smartphones. Most recent reports show that the malicious applications are rapidly increasing for Android based smartphones. The assessment of various threats and vulnerabilities and lack of effective mechanisms to identify malicious applications calls for implementation of security measures. The vulnerabilities introduced by libraries in the Android software stack such as Stage fright multimedia library have been analyzed. It allows an attacker to attack via heap overflow that could leak sensitive data without internet permissions. Some mechanisms to prevent attack such as hardening the memory-mapping in Android devices are proposed. Ubiquitous nature of smartphones leads to storing confidential personal information necessitating the need for securing such information in the case of loss of device. A tool that uses a lightweight authenticated encryption algorithm, Hummingbird-2 has been developed to secure the information stored. It is resistant to most attacks applicable to block and stream ciphers. Another research is focused towards malware detection methods. The signature based techniques are ineffective in detecting zero day malwares. An improved malware detection technique has been proposed which uses a hybrid framework based on permissions and intents. Classification is done by applying machine learning methods using WEKA tool. Experiments on the dataset reveal that the hybrid framework achieved an average of 0.9 AUC. Another approach introduces a novel method to reliably identify the semantic similarity between two programs through the use of function call graphs. It uses a labelling function inspired by the neighborhood hash graph kernel to represent malicious behaviors. Evolutionary algorithms such as particle swarm optimization (PSO) have proven to be effective in optimized feature selection for efficient classification. Cultural Cooperative Particle Swarm Optimization ANFIS (CCPSO-ANFIS) system have been proposed. The results reveal the proposed method achieved 98.2% accuracy in detecting Android malware

Contents

1. Introduction 2. Structuring android threats and attack vectors 3. Lightweight encryption for android based mobile devices 4. Analysis of Android malware 5. Structural detection of android malware using function call graphs 6. An intelligent mobile malware CCPSO-ANFIS based classifier system 7. Conclusion and future work.