



IJCSI

International Journal of Computer Science Issues

Volume 7, Issue 3, No 9, May 2010
ISSN (Online): 1694-0784
ISSN (Print): 1694-0814

© IJCSI PUBLICATION
www.IJCSI.org

IJCSI proceedings are currently indexed by:



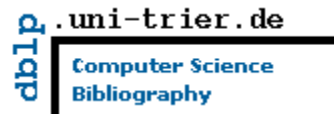
Cogprints

Google scholar



SciRate.com

CiteSeer^x beta



DOAJ DIRECTORY OF
OPEN ACCESS
JOURNALS



ProQuest

IJCSI Publicity Board 2010

Dr. Borislav D Dimitrov

Department of General Practice, Royal College of Surgeons in Ireland
Dublin, Ireland

Dr. Vishal Goyal

Department of Computer Science, Punjabi University
Patiala, India

Mr. Nehinbe Joshua

University of Essex
Colchester, Essex, UK

Mr. Vassilis Papataxiarhis

Department of Informatics and Telecommunications
National and Kapodistrian University of Athens, Athens, Greece

EDITORIAL

In this third edition of 2010, we bring forward issues from various dynamic computer science areas ranging from system performance, computer vision, artificial intelligence, software engineering, multimedia , pattern recognition, information retrieval, databases, security and networking among others.

As always we thank all our reviewers for providing constructive comments on papers sent to them for review. This helps enormously in improving the quality of papers published in this issue.

IJCSI will maintain its policy of sending print copies of the journal to all corresponding authors worldwide free of charge. Apart from availability of the full-texts from the journal website, all published papers are deposited in open-access repositories to make access easier and ensure continuous availability of its proceedings.

The transition from the 2nd issue to the 3rd one has been marked with an agreement signed between **IJCSI** and **ProQuest** and **EBSCOHOST**, two leading directories to help in the dissemination of our published papers. We believe further indexing and more dissemination will definitely lead to further citations of our authors' articles.

We are pleased to present IJCSI Volume 7, Issue 3, May 2010, split in eleven numbers (IJCSI Vol. 7, Issue 3, No. 9). The acceptance rate for this issue is 37.88%.

We wish you a happy reading!

IJCSI Editorial Board
May 2010 Issue
ISSN (Print): 1694-0814
ISSN (Online): 1694-0784
© IJCSI Publications
www.IJCSI.org

IJCSI Editorial Board 2010

Dr Tristan Vanrullen

Chief Editor

LPL, Laboratoire Parole et Langage - CNRS - Aix en Provence, France

LABRI, Laboratoire Bordelais de Recherche en Informatique - INRIA - Bordeaux, France

LEEE, Laboratoire d'Esthétique et Expérimentations de l'Espace - Université d'Auvergne, France

Dr Constantino Malagón

Associate Professor

Nebrija University

Spain

Dr Lamia Fourati Chaari

Associate Professor

Multimedia and Informatics Higher Institute in SFAX

Tunisia

Dr Mokhtar Beldjehem

Professor

Sainte-Anne University

Halifax, NS, Canada

Dr Pascal Chatonnay

Assistant Professor

Maître de Conférences

Laboratoire d'Informatique de l'Université de Franche-Comté

Université de Franche-Comté

France

Dr Yee-Ming Chen

Professor

Department of Industrial Engineering and Management

Yuan Ze University

Taiwan

Dr Vishal Goyal

Assistant Professor
Department of Computer Science
Punjabi University
Patiala, India

Dr Natarajan Meghanathan

Assistant Professor
REU Program Director
Department of Computer Science
Jackson State University
Jackson, USA

Dr Deepak Laxmi Narasimha

Department of Software Engineering,
Faculty of Computer Science and Information Technology,
University of Malaya,
Kuala Lumpur, Malaysia

Dr Navneet Agrawal

Assistant Professor
Department of ECE,
College of Technology & Engineering,
MPUAT, Udaipur 313001 Rajasthan, India

Prof N. Jaisankar

Assistant Professor
School of Computing Sciences,
VIT University
Vellore, Tamilnadu, India

IJCSI Reviewers Committee 2010

- Mr. Markus Schatten, University of Zagreb, Faculty of Organization and Informatics, Croatia
- Mr. Vassilis Papataxiarhis, Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Athens, Greece
- Dr Modestos Stavrakis, University of the Aegean, Greece
- Dr Fadi KHALIL, LAAS -- CNRS Laboratory, France
- Dr Dimitar Trajanov, Faculty of Electrical Engineering and Information technologies, ss. Cyril and Methodius Univesity - Skopje, Macedonia
- Dr Jinping Yuan, College of Information System and Management,National Univ. of Defense Tech., China
- Dr Alexis Lazanas, Ministry of Education, Greece
- Dr Stavroula Mougiakakou, University of Bern, ARTORG Center for Biomedical Engineering Research, Switzerland
- Dr Cyril de Runz, CReSTIC-SIC, IUT de Reims, University of Reims, France
- Mr. Pramodkumar P. Gupta, Dept of Bioinformatics, Dr D Y Patil University, India
- Dr Alireza Fereidunian, School of ECE, University of Tehran, Iran
- Mr. Fred Viezens, Otto-Von-Guericke-University Magdeburg, Germany
- Dr. Richard G. Bush, Lawrence Technological University, United States
- Dr. Ola Osunkoya, Information Security Architect, USA
- Mr. Kotsokostas N.Antonios, TEI Piraeus, Hellas
- Prof Steven Totosy de Zepetnek, U of Halle-Wittenberg & Purdue U & National Sun Yat-sen U, Germany, USA, Taiwan
- Mr. M Arif Siddiqui, Najran University, Saudi Arabia
- Ms. Ilknur Icke, The Graduate Center, City University of New York, USA
- Prof Miroslav Baca, Faculty of Organization and Informatics, University of Zagreb, Croatia
- Dr. Elvia Ruiz Beltrán, Instituto Tecnológico de Aguascalientes, Mexico
- Mr. Moustafa Banbouk, Engineer du Telecom, UAE
- Mr. Kevin P. Monaghan, Wayne State University, Detroit, Michigan, USA
- Ms. Moira Stephens, University of Sydney, Australia
- Ms. Maryam Feily, National Advanced IPv6 Centre of Excellence (NAV6) , Universiti Sains Malaysia (USM), Malaysia
- Dr. Constantine YIALOURIS, Informatics Laboratory Agricultural University of Athens, Greece
- Mrs. Angeles Abella, U. de Montreal, Canada
- Dr. Patrizio Arrigo, CNR ISMAC, italy
- Mr. Anirban Mukhopadhyay, B.P.Poddar Institute of Management & Technology, India
- Mr. Dinesh Kumar, DAV Institute of Engineering & Technology, India
- Mr. Jorge L. Hernandez-Ardieta, INDRA SISTEMAS / University Carlos III of Madrid, Spain
- Mr. AliReza Shahrestani, University of Malaya (UM), National Advanced IPv6 Centre of Excellence (NAv6), Malaysia
- Mr. Blagoj Ristevski, Faculty of Administration and Information Systems Management - Bitola, Republic of Macedonia
- Mr. Mauricio Egidio Cantão, Department of Computer Science / University of São Paulo, Brazil
- Mr. Jules Ruis, Fractal Consultancy, The Netherlands

- Mr. Mohammad Iftekhar Husain, University at Buffalo, USA
- Dr. Deepak Laxmi Narasimha, Department of Software Engineering, Faculty of Computer Science and Information Technology, University of Malaya, Malaysia
- Dr. Paola Di Maio, DMEM University of Strathclyde, UK
- Dr. Bhanu Pratap Singh, Institute of Instrumentation Engineering, Kurukshetra University Kurukshetra, India
- Mr. Sana Ullah, Inha University, South Korea
- Mr. Cornelis Pieter Pieters, Condast, The Netherlands
- Dr. Amogh Kavimandan, The MathWorks Inc., USA
- Dr. Zhinan Zhou, Samsung Telecommunications America, USA
- Mr. Alberto de Santos Sierra, Universidad Politécnica de Madrid, Spain
- Dr. Md. Atiqur Rahman Ahad, Department of Applied Physics, Electronics & Communication Engineering (APECE), University of Dhaka, Bangladesh
- Dr. Charalampos Bratsas, Lab of Medical Informatics, Medical Faculty, Aristotle University, Thessaloniki, Greece
- Ms. Alexia Dini Kounoudes, Cyprus University of Technology, Cyprus
- Mr. Anthony Gesase, University of Dar es salaam Computing Centre, Tanzania
- Dr. Jorge A. Ruiz-Vanoye, Universidad Juárez Autónoma de Tabasco, Mexico
- Dr. Alejandro Fuentes Penna, Universidad Popular Autónoma del Estado de Puebla, México
- Dr. Ocotlán Díaz-Parra, Universidad Juárez Autónoma de Tabasco, México
- Mrs. Nantia Iakovidou, Aristotle University of Thessaloniki, Greece
- Mr. Vinay Chopra, DAV Institute of Engineering & Technology, Jalandhar
- Ms. Carmen Lastres, Universidad Politécnica de Madrid - Centre for Smart Environments, Spain
- Dr. Sanja Lazarova-Molnar, United Arab Emirates University, UAE
- Mr. Srikrishna Nudurumati, Imaging & Printing Group R&D Hub, Hewlett-Packard, India
- Dr. Olivier Nocent, CReSTIC/SIC, University of Reims, France
- Mr. Burak Cizmeci, Isik University, Turkey
- Dr. Carlos Jaime Barrios Hernandez, LIG (Laboratory Of Informatics of Grenoble), France
- Mr. Md. Rabiul Islam, Rajshahi university of Engineering & Technology (RUET), Bangladesh
- Dr. LAKHOUA Mohamed Najeh, ISSAT - Laboratory of Analysis and Control of Systems, Tunisia
- Dr. Alessandro Lavacchi, Department of Chemistry - University of Firenze, Italy
- Mr. Mungwe, University of Oldenburg, Germany
- Mr. Somnath Tagore, Dr D Y Patil University, India
- Ms. Xueqin Wang, ATCS, USA
- Dr. Borislav D Dimitrov, Department of General Practice, Royal College of Surgeons in Ireland, Dublin, Ireland
- Dr. Fondjo Fotou Franklin, Langston University, USA
- Dr. Vishal Goyal, Department of Computer Science, Punjabi University, Patiala, India
- Mr. Thomas J. Clancy, ACM, United States
- Dr. Ahmed Nabih Zaki Rashed, Dr. in Electronic Engineering, Faculty of Electronic Engineering, menouf 32951, Electronics and Electrical Communication Engineering Department, Menoufia university, EGYPT, EGYPT
- Dr. Rushed Kanawati, LIPN, France
- Mr. Koteswar Rao, K G Reddy College Of ENGG.&TECH,CHILKUR, RR DIST.,AP, India

- Mr. M. Nagesh Kumar, Department of Electronics and Communication, J.S.S. research foundation, Mysore University, Mysore-6, India
- Dr. Ibrahim Noha, Grenoble Informatics Laboratory, France
- Mr. Muhammad Yasir Qadri, University of Essex, UK
- Mr. Annadurai .P, KMCPGS, Lawspet, Pondicherry, India, (Aff. Pondicherry Univeristy, India)
- Mr. E Munivel , CEDTI (Govt. of India), India
- Dr. Chitra Ganesh Desai, University of Pune, India
- Mr. Syed, Analytical Services & Materials, Inc., USA
- Dr. Mashud Kabir, Department of Computer Science, University of Tuebingen, Germany
- Mrs. Payal N. Raj, Veer South Gujarat University, India
- Mrs. Priti Maheshwary, Maulana Azad National Institute of Technology, Bhopal, India
- Mr. Mahesh Goyani, S.P. University, India, India
- Mr. Vinay Verma, Defence Avionics Research Establishment, DRDO, India
- Dr. George A. Papakostas, Democritus University of Thrace, Greece
- Mr. Abhijit Sanjiv Kulkarni, DARE, DRDO, India
- Mr. Kavi Kumar Khedo, University of Mauritius, Mauritius
- Dr. B. Sivaselvan, Indian Institute of Information Technology, Design & Manufacturing, Kancheepuram, IIT Madras Campus, India
- Dr. Partha Pratim Bhattacharya, Greater Kolkata College of Engineering and Management, West Bengal University of Technology, India
- Mr. Manish Maheshwari, Makhanlal C University of Journalism & Communication, India
- Dr. Siddhartha Kumar Khaitan, Iowa State University, USA
- Dr. Mandhapati Raju, General Motors Inc, USA
- Dr. M.Iqbal Saripan, Universiti Putra Malaysia, Malaysia
- Mr. Ahmad Shukri Mohd Noor, University Malaysia Terengganu, Malaysia
- Mr. Selvakuberan K, TATA Consultancy Services, India
- Dr. Smita Rajpal, Institute of Technology and Management, Gurgaon, India
- Mr. Rakesh Kachroo, Tata Consultancy Services, India
- Mr. Raman Kumar, National Institute of Technology, Jalandhar, Punjab., India
- Mr. Nitesh Sureja, S.P.University, India
- Dr. M. Emre Celebi, Louisiana State University, Shreveport, USA
- Dr. Aung Kyaw Oo, Defence Services Academy, Myanmar
- Mr. Sanjay P. Patel, Sankalchand Patel College of Engineering, Visnagar, Gujarat, India
- Dr. Pascal Fallavollita, Queens University, Canada
- Mr. Jitendra Agrawal, Rajiv Gandhi Technological University, Bhopal, MP, India
- Mr. Ismael Rafael Ponce Medellín, Cenidet (Centro Nacional de Investigación y Desarrollo Tecnológico), Mexico
- Mr. Supheakmunkol SARIN, Waseda University, Japan
- Mr. Shoukat Ullah, Govt. Post Graduate College Bannu, Pakistan
- Dr. Vivian Augustine, Telecom Zimbabwe, Zimbabwe
- Mrs. Mutalli Vatile, Offshore Business Philipines, Philipines
- Dr. Emanuele Goldoni, University of Pavia, Dept. of Electronics, TLC & Networking Lab, Italy
- Mr. Pankaj Kumar, SAMA, India
- Dr. Himanshu Aggarwal, Punjabi University,Patiala, India
- Dr. Vauvert Guillaume, Europages, France

- Prof Yee Ming Chen, Department of Industrial Engineering and Management, Yuan Ze University, Taiwan
- Dr. Constantino Malagón, Nebrija University, Spain
- Prof Kanwalvir Singh Dhindsa, B.B.S.B.Engg.College, Fatehgarh Sahib (Punjab), India
- Mr. Angkoon Phinyomark, Prince of Singkla University, Thailand
- Ms. Nital H. Mistry, Veer Narmad South Gujarat University, Surat, India
- Dr. M.R.Sumalatha, Anna University, India
- Mr. Somesh Kumar Dewangan, Disha Institute of Management and Technology, India
- Mr. Raman Maini, Punjabi University, Patiala(Punjab)-147002, India
- Dr. Abdelkader Outtagarts, Alcatel-Lucent Bell-Labs, France
- Prof Dr. Abdul Wahid, AKG Engg. College, Ghaziabad, India
- Mr. Prabu Mohandas, Anna University/Adhityamaan College of Engineering, india
- Dr. Manish Kumar Jindal, Panjab University Regional Centre, Muktsar, India
- Prof Mydhili K Nair, M S Ramaiah Institute of Technnology, Bangalore, India
- Dr. C. Suresh Gnana Dhas, VelTech MultiTech Dr.Rangarajan Dr.Sagunthala Engineering College,Chennai,Tamilnadu, India
- Prof Akash Rajak, Krishna Institute of Engineering and Technology, Ghaziabad, India
- Mr. Ajay Kumar Shrivastava, Krishna Institute of Engineering & Technology, Ghaziabad, India
- Mr. Deo Prakash, SMVD University, Kakryal(J&K), India
- Dr. Vu Thanh Nguyen, University of Information Technology HoChiMinh City, VietNam
- Prof Deo Prakash, SMVD University (A Technical University open on I.I.T. Pattern) Kakryal (J&K), India
- Dr. Navneet Agrawal, Dept. of ECE, College of Technology & Engineering, MPUAT, Udaipur 313001 Rajasthan, India
- Mr. Sufal Das, Sikkim Manipal Institute of Technology, India
- Mr. Anil Kumar, Sikkim Manipal Institute of Technology, India
- Dr. B. Prasanalakshmi, King Saud University, Saudi Arabia.
- Dr. K D Verma, S.V. (P.G.) College, Aligarh, India
- Mr. Mohd Nazri Ismail, System and Networking Department, University of Kuala Lumpur (UniKL), Malaysia
- Dr. Nguyen Tuan Dang, University of Information Technology, Vietnam National University Ho Chi Minh city, Vietnam
- Dr. Abdul Aziz, University of Central Punjab, Pakistan
- Dr. P. Vasudeva Reddy, Andhra University, India
- Mrs. Savvas A. Chatzichristofis, Democritus University of Thrace, Greece
- Mr. Marcio Dorn, Federal University of Rio Grande do Sul - UFRGS Institute of Informatics, Brazil
- Mr. Luca Mazzola, University of Lugano, Switzerland
- Mr. Nadeem Mahmood, Department of Computer Science, University of Karachi, Pakistan
- Mr. Hafeez Ullah Amin, Kohat University of Science & Technology, Pakistan
- Dr. Professor Vikram Singh, Ch. Devi Lal University, Sirsa (Haryana), India
- Mr. M. Azath, Calicut/Mets School of Enginerring, India
- Dr. J. Hanumanthappa, DoS in CS, University of Mysore, India
- Dr. Shahanawaj Ahamad, Department of Computer Science, King Saud University, Saudi Arabia
- Dr. K. Duraiswamy, K. S. Rangasamy College of Technology, India
- Prof. Dr Mazlina Esa, Universiti Teknologi Malaysia, Malaysia

- Dr. P. Vasant, Power Control Optimization (Global), Malaysia
- Dr. Taner Tuncer, Firat University, Turkey
- Dr. Norrozila Sulaiman, University Malaysia Pahang, Malaysia
- Prof. S K Gupta, BCET, Guradspur, India
- Dr. Latha Parameswaran, Amrita Vishwa Vidyapeetham, India
- Mr. M. Azath, Anna University, India
- Dr. P. Suresh Varma, Adikavi Nannaya University, India
- Prof. V. N. Kamalesh, JSS Academy of Technical Education, India
- Dr. D Gunaseelan, Ibri College of Technology, Oman
- Mr. Sanjay Kumar Anand, CDAC, India
- Mr. Akshat Verma, CDAC, India
- Mrs. Fazeela Tunnisa, Najran University, Kingdom of Saudi Arabia
- Mr. Hasan Asil, Islamic Azad University Tabriz Branch (Azarshahr), Iran
- Prof. Dr Sajal Kabiraj, Fr. C Rodrigues Institute of Management Studies (Affiliated to University of Mumbai, India), India
- Mr. Syed Fawad Mustafa, GAC Center, Shandong University, China
- Dr. Natarajan Meghanathan, Jackson State University, Jackson, MS, USA
- Prof. Selvakani Kandeegan, Francis Xavier Engineering College, India
- Mr. Tohid Sedghi, Urmia University, Iran
- Dr. S. Sasikumar, PSNA College of Engg and Tech, Dindigul, India
- Dr. Anupam Shukla, Indian Institute of Information Technology and Management Gwalior, India
- Mr. Rahul Kala, Indian Institute of Information Technology and Management Gwalior, India
- Dr. A V Nikolov, National University of Lesotho, Lesotho
- Mr. Kamal Sarkar, Department of Computer Science and Engineering, Jadavpur University, India
- Dr. Mokhled S. Altarawneh, Computer Engineering Dept., Faculty of Engineering, Mutah University, Jordan, Jordan
- Prof. Sattar J Aboud, Iraqi Council of Representatives, Iraq-Baghdad
- Dr. Prasant Kumar Pattnaik, Department of CSE, KIST, India
- Dr. Mohammed Amoon, King Saud University, Saudi Arabia
- Dr. Tsvetanka Georgieva, Department of Information Technologies, St. Cyril and St. Methodius University of Veliko Tarnovo, Bulgaria
- Dr. Eva Volna, University of Ostrava, Czech Republic
- Mr. Ujjal Marjit, University of Kalyani, West-Bengal, India
- Dr. Prasant Kumar Pattnaik, KIST, Bhubaneswar, India, India
- Dr. Guezouri Mustapha, Department of Electronics, Faculty of Electrical Engineering, University of Science and Technology (USTO), Oran, Algeria
- Mr. Maniyar Shiraz Ahmed, Najran University, Najran, Saudi Arabia
- Dr. Sreedhar Reddy, JNTU, SSIIETW, Hyderabad, India
- Mr. Bala Dhandayuthapani Veerasamy, Mekelle University, Ethiopia
- Mr. Arash Habibi Lashkari, University of Malaya (UM), Malaysia
- Mr. Rajesh Prasad, LDC Institute of Technical Studies, Allahabad, India
- Ms. Habib Izadkhah, Tabriz University, Iran
- Dr. Lokesh Kumar Sharma, Chhattisgarh Swami Vivekanand Technical University Bhilai, India
- Mr. Kuldeep Yadav, IIIT Delhi, India
- Dr. Naoufel Kraiem, Institut Supérieur d'Informatique, Tunisia

- Prof. Frank Ortmeier, Otto-von-Guericke-Universitaet Magdeburg, Germany
- Mr. Ashraf Aljammal, USM, Malaysia
- Mrs. Amandeep Kaur, Department of Computer Science, Punjabi University, Patiala, Punjab, India
- Mr. Babak Basharirad, University Technology of Malaysia, Malaysia
- Mr. Avinash singh, Kiet Ghaziabad, India
- Dr. Miguel Vargas-Lombardo, Technological University of Panama, Panama
- Dr. Tuncay Sevindik, Firat University, Turkey
- Ms. Pavai Kandavelu, Anna University Chennai, India
- Mr. Ravish Khichar, Global Institute of Technology, India
- Mr AOs Alaa Zaidan Ansaef, Multimedia University, Cyberjaya, Malaysia
- Dr. Awadhesh Kumar Sharma, Dept. of CSE, MMM Engg College, Gorakhpur-273010, UP, India
- Mr. Qasim Siddique, FUIEMS, Pakistan
- Dr. Le Hoang Thai, University of Science, Vietnam National University - Ho Chi Minh City, Vietnam
- Dr. Saravanan C, NIT, Durgapur, India
- Dr. Vijay Kumar Mago, DAV College, Jalandhar, India
- Dr. Do Van Nhon, University of Information Technology, Vietnam
- Mr. Georgios Kioumourtzis, University of Patras, Greece
- Mr. Amol D.Potgantwar, SITRC Nasik, India
- Mr. Lesedi Melton Masisi, Council for Scientific and Industrial Research, South Africa
- Dr. Karthik.S, Department of Computer Science & Engineering, SNS College of Technology, India
- Mr. Nafiz Imtiaz Bin Hamid, Department of Electrical and Electronic Engineering, Islamic University of Technology (IUT), Bangladesh
- Mr. Muhammad Imran Khan, Universiti Teknologi PETRONAS, Malaysia
- Dr. Abdul Kareem M. Radhi, Information Engineering - Nahrin University, Iraq
- Dr. Mohd Nazri Ismail, University of Kuala Lumpur, Malaysia
- Dr. Manuj Darbari, BBDNITM, Institute of Technology, A-649, Indira Nagar, Lucknow 226016, India
- Ms. Izerrouken, INP-IRIT, France
- Mr. Nitin Ashokrao Naik, Dept. of Computer Science, Yeshwant Mahavidyalaya, Nanded, India
- Mr. Nikhil Raj, National Institute of Technology, Kurukshetra, India
- Prof. Maher Ben Jemaa, National School of Engineers of Sfax, Tunisia
- Prof. Rajeshwar Singh, BRCM College of Engineering and Technology, Bahal Bhiwani, Haryana, India
- Mr. Gaurav Kumar, Department of Computer Applications, Chitkara Institute of Engineering and Technology, Rajpura, Punjab, India
- Mr. Ajeet Kumar Pandey, Indian Institute of Technology, Kharagpur, India
- Mr. Rajiv Phougat, IBM Corporation, USA
- Mrs. Aysha V, College of Applied Science Pattuvam affiliated with Kannur University, India
- Dr. Debotosh Bhattacharjee, Department of Computer Science and Engineering, Jadavpur University, Kolkata-700032, India
- Dr. Neelam Srivastava, Institute of engineering & Technology, Lucknow, India
- Prof. Sweta Verma, Galgotia's College of Engineering & Technology, Greater Noida, India
- Mr. Harminder Singh BIndra, MIMIT, INDIA
- Dr. Lokesh Kumar Sharma, Chhattisgarh Swami Vivekanand Technical University, Bhilai, India
- Mr. Tarun Kumar, U.P. Technical University/Radha Govinend Engg. College, India
- Mr. Tirthraj Rai, Jawahar Lal Nehru University, New Delhi, India

- Mr. Akhilesh Tiwari, Madhav Institute of Technology & Science, India
- Mr. Dakshina Ranjan Kisku, Dr. B. C. Roy Engineering College, WBUT, India
- Ms. Anu Suneja, Maharshi Markandeshwar University, Mullana, Haryana, India
- Mr. Munish Kumar Jindal, Punjabi University Regional Centre, Jaito (Faridkot), India
- Dr. Ashraf Bany Mohammed, Management Information Systems Department, Faculty of Administrative and Financial Sciences, Petra University, Jordan
- Mrs. Jyoti Jain, R.G.P.V. Bhopal, India
- Dr. Lamia Chaari, SFAX University, Tunisia
- Mr. Akhter Raza Syed, Department of Computer Science, University of Karachi, Pakistan
- Prof. Khubaib Ahmed Qureshi, Information Technology Department, HIMS, Hamdard University, Pakistan
- Prof. Boubker Sbihi, Ecole des Sciences de L'Information, Morocco
- Dr. S. M. Riazul Islam, Inha University, South Korea
- Prof. Lokhande S.N., S.R.T.M. University, Nanded (MH), India
- Dr. Vijay H Mankar, Dept. of Electronics, Govt. Polytechnic, Nagpur, India
- Dr. M. Sreedhar Reddy, JNTU, Hyderabad, SSIETW, India
- Mr. Ojesanmi Olusegun, Ajayi Crowther University, Oyo, Nigeria
- Ms. Mamta Juneja, RBIEBT, PTU, India
- Dr. Ekta Walia Bhullar, Maharishi Markandeshwar University, Mullana Ambala (Haryana), India
- Prof. Chandra Mohan, John Bosco Engineering College, India
- Mr. Nitin A. Naik, Yeshwant Mahavidyalaya, Nanded, India
- Mr. Sunil Kashibarao Nayak, Bahirji Smarak Mahavidyalaya, Basmathnagar Dist-Hingoli., India
- Prof. Rakesh.L, Vijetha Institute of Technology, Bangalore, India
- Mr B. M. Patil, Indian Institute of Technology, Roorkee, Uttarakhand, India
- Mr. Thipendra Pal Singh, Sharda University, K.P. III, Greater Noida, Uttar Pradesh, India
- Prof. Chandra Mohan, John Bosco Engg College, India
- Mr. Hadi Saboohi, University of Malaya - Faculty of Computer Science and Information Technology, Malaysia
- Dr. R. Baskaran, Anna University, India
- Dr. Wichian Sittiprapaporn, Mahasarakham University College of Music, Thailand
- Mr. Lai Khin Wee, Universiti Teknologi Malaysia, Malaysia
- Dr. Kamaljit I. Lakhtaria, Atmiya Institute of Technology, India
- Mrs. Inderpreet Kaur, PTU, Jalandhar, India
- Mr. Iqbaldeep Kaur, PTU / RBIEBT, India
- Mrs. Vasudha Bahl, Maharaja Agrasen Institute of Technology, Delhi, India
- Prof. Vinay Uttamrao Kale, P.R.M. Institute of Technology & Research, Badnera, Amravati, Maharashtra, India
- Mr. Suhas J Manangi, Microsoft, India
- Ms. Anna Kuzio, Adam Mickiewicz University, School of English, Poland
- Dr. Debojyoti Mitra, Sir Padampat Singhania University, India
- Prof. Rachit Garg, Department of Computer Science, L K College, India
- Mrs. Manjula K A, Kannur University, India
- Mr. Rakesh Kumar, Indian Institute of Technology Roorkee, India

TABLE OF CONTENTS

- 1. A Coded Cooperative Networking MAC protocol in non transparent multihop WiMAX network** **Pg 1-9**
Lamia Chaari, Lotfi Kamoun

- 2. Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography** **Pg 10-16**
Wilayat Khan, Habib Ullah

- 3. Touching Syllable Segmentation using Split Profile Algorithm** **Pg 17-26**
L.Pratap Reddy, T.Ranga Babu, N.Venkata Rao, B.Raveendra Babu

- 4. Information Security and Sender's Rights Protection through Embedded Public Key Signature** **Pg 27-34**
Vineeta Khemchandani, G. N. Purohit

- 5. Non linear Image segmentation using fuzzy c means clustering method with thresholding for underwater images** **Pg 35-40**
G. Padmavathi, M. Muthukumar, Suresh Kumar Thakur

- 6. A Theoretical Approach to Link Mining for personalization** **Pg 41-44**
K. Srinivas, L. Kiran Kumar Reddy, A. Govardhan

- 7. Image Compression Algorithms for Fingerprint System** **Pg 45-50**
Preeti Pathak

A Coded Cooperative Networking MAC protocol in non transparent multihop WiMAX network

Lamia CHAARI, Lotfi KAMOUN

University of SFAX, Electronic and Technology Information Laboratory, TUNISIA

Abstract

IEEE 802.16j mobile multi-hop relay (MMR) was proposed to gain coverage extension and throughput enhancement. The objective of this work, is to suggest a coded cooperative networking MAC protocol in non transparent multihop WiMax network. The proposed design takes in consideration network coding approach between relays. We try to address the division of an IEEE 802.16j frame into different zones. We suggest a frame structure that supports 3 hops non transparent TTR mode. Related work and the 802.16j capability are also deeply discussed.

Keywords: Cooperative, network coding, frame, multihop, IEEE 802.16j, MAC.

1. Introduction

Cooperative communication (CooCom) [1, 2, 3, 4, 5, 53] is a recent paradigm for wireless relay networks [6, 7, 8, 9, 10], proposed as a way to improve wireless network reliability and capacity. The main technical benefits coming along with cooperative communications are higher coverage, improved spectrum usage, lower energy consumption, increased location estimation accuracy, etc.). The broadcast nature of the wireless medium is the main enabler of cooperative communications.

Cocom enables single-antenna nodes in a multi-user environment to share their resources to jointly transmit information in order to achieve an improvement in overall performance and reap some of the benefits of multiple-input, multiple-output (MIMO) [11, 50, 51] systems. The classical relay channel model [6,12,13,14, 21, 52] is comprised of three terminals a source that transmits information, a destination that receives information, and a relay that both receives and transmits information in order to enhance communication between the source and destination. Cooperation is a generalization of the relay channel to multiple sources with information to transmit that also serve as relays for each other. Combinations of relaying and cooperation are known as cooperative communications.

This is realized via the application of cooperative diversity techniques that take advantage of the spatial

diversity offered by cooperation between wireless terminals. Diversity increases capacity and provides robustness against fading. The most common diversity methods are spatial diversity using multiple antennas, temporal diversity using automatic repeat request schemes or block interleaving with error correction, and frequency diversity using frequency spreading, frequency hopping, or orthogonal frequency division multiplexing techniques. Cooperative diversity refers to the class of techniques where diversity benefits are gained via the sharing of information between multiple cooperating terminals in a wireless network. Several relaying cooperative strategies [15] for wireless relay networks are proposed:

- decode-and-forward [17, 18],
- amplify-and-forward [19, 47],
- compress-and-forward [20],
- selection relaying scheme [16, 22→ 25].
- opportunistic relaying scheme[16, 26],
- coded cooperation (CC) [27, 28],
- Space-time CC [29, 30]

In decode and forward method a cooperating node first decodes signals received from a source and then relays or retransmits them. The receiver at the destination uses information retransmitted from multiple relays and the source (when available) to make decisions. Perfect regeneration at the relays may require retransmission of symbols or use of forward error correction (FEC) depending on the quality of the channel between the source and the relays. This may not be suitable for a delay limited networks. In amplify and forward each cooperating node receives the signals transmitted by the source node but don't decode them. These signals in their noisy form are amplified to compensate for the attenuation suffered between the source-to-relay links and retransmitted. The destination requires knowledge of the channel state between source-to-relay links to correctly decode the symbols sent from the source.

In compress and forward the received signal is only quantized instead of being fully decoded, the quantized symbols are not directly repeated in phase 2 they are compressed by Wyner-Ziv coding [31]. The selection

relaying schemes choose the strategy with best performance based upon channel measurements between the cooperating terminals. In an opportunistic relaying scheme (ORS) only the best relay is allowed to cooperate with the source. If channel conditions are not statistically equal for all relays, ORS may be unfair among relays. That is, relays with the worst channel conditions are never selected and all the cooperation is performed by a reduced set of relays. This can induce a negative effect in the network behavior as one (or more) relays can waste all the battery energy for the sake of cooperation.

The coded cooperation provides cooperation diversity by distributed Forward Error Correction (FEC) coding and considers the result of the error check for its relaying decision. If a user is not able to correctly decode the partner's bits it forwards its own data during the second phase. The Space-time CC exploit spatial diversity available among a collection of distributed terminals that relay messages for one another in such a manner that the destination terminal can average the fading, even though it is unknown a priori which terminals will be involved. In particular, a source initiates transmission to its destination, and many relays potentially receive the transmission. Those terminals that can fully decode the transmission utilize a space-time code to cooperatively relay to the destination.

Many other strategies have been proposed. In [32] new cooperative strategy for ad hoc networks that are more spectrally efficient than classical Decode & Forward (DF) protocols was proposed. Using analog network coding was suggested in order to improve spectral efficiency of the cooperative system by relaxing the orthogonally constraint, though preserving the practical half-duplex constraint.

Although all these schemes employ different techniques to process the relayed data, all of them employ at least two phases per cooperation cycle separated for the reason that wireless terminals cannot transmit and receive simultaneously at the same time and frequency. While in the first phase the users exchange their data, in the second phase the users help each other by relaying the data/signal. The emerging IEEE 802.16j standard may allow w/o relay transmissions in the second phase.

The cooperative connectivity of a wireless relay network is defined as the set of communication links between pairs of terminals that are used in the transmission of an information signal from a source terminal to a destination terminal. Relay terminals are defined to cooperate with the source terminal when they transmit a signal that helps the destination terminal to successfully decode the original information signal. The ways that cooperating terminals can be connected to each other in wireless relay networks, the constraints imposed by the availability of different system resources and the

achievable combinations of communication links between cooperating terminals are also deeply presented in the literature [54].

Recently, network coding [33, 34, 35,] as well has received a lot of attention for its potential advantages in improving throughput and enhancing robustness for multi-source systems. The basic principle of network coding is to linearly combine multiple independent information flows into one flow to transmit. There have been several proposals for applying network coding to multi-source relaying networks, with or without cooperation. The interaction between Cooperation and Network Coding [36] has recently received a significant deal of attention, as a combination of the two brings novelty, flexibility and improved performance. However, there is a lack of studies about real-world scenarios.

Multihop relaying is already part of the standards currently being developed for wireless broadband systems [37] such as 802.16j [38] and 802.16m [39], which is an indication of growing consensus on the effectiveness of cooperative communication. However, at this stage, there are many open issues regarding good 802.16j relay network solutions:

- While there have been a few initial studies on IEEE 802.16j MMR networks, not much is really known about the performance of such systems. This makes it very difficult to have clear ideas of the potential of this technology.
- The current standard does not specify how the radio resource allocation will be done.
- Some initial studies on the design of 802.16j system have been carried out. The issues relative to the planning of multiple relays is still open.

No previous work has specifically look to the implementations issues of a coded cooperative networking MAC protocol over 802.16j systems. More specifically, the focus of this contribution is to propose a coded cooperative networking MAC protocol in fixed broadband wireless access systems with multihop relay Wimax networks, which we denoted it CCNMAC_{MHRwimax} "Coded Cooperative Networking MAC protocol for Multihop Relay Wimax networks". Such proposal require firstly a deep research on coding schemes [40, 41] used for combining, on relaying techniques used for mutually exchanging data, on multiple access methods to limit interference and overhead, on cooperation aware resource allocation such as selecting partners[42, 43] and cooperation level [44, 45] , on routing methods [46] in multi-hop cooperative networks. Secondly we must focus on the practical issues for cooperative networking when trying to apply cooperation in an existing standard, such as IEEE 802.16j networks.

Researches on cooperative mechanisms at MAC layer are commonly related to WLAN networks [55, 56, 57, 58] and only some works for WMAN networks [59,60].

In [61] the authors propose A user scheduling and radio resource allocation algorithm for two-hop wireless relay networks in order to efficiently integrate various cooperative diversity schemes for the emerging IEEE 802.16j based systems. The analysis of the system with this scheduler shows that a simple cooperative diversity scheme which dynamically selects the best scheme between conventional relaying and direct transmission is promising in terms of throughput and implementation complexity.

The paper is organized as follows. In this section we have briefly reviewed related work. A reasonably detailed description of the 802.16j capability based on the current draft is presented in section 2. In Section 3, Frame structure for MMR in non transparent mode with tunneling and network coding approach is proposed. Finally, the paper is concluded in section 4.

2. IEEE 802.16j capabilities

The IEEE 802.16j is an amendment to the IEEE 802.16e standard to enable the functionalities of interoperable RSs and BSs. The IEEE 802.16j standard is currently being developed for increasing the coverage area of the IEEE 802.16e standard via the deployment of fixed or nomadic relay terminals.

In this section, the key system features and the capabilities of the IEEE 802.16j MR network are overviewed. The discussion will focus on two particular aspects the different relay modes that are defined and the frame structure that is proposed.

2.1 Relay mode

The basic system architecture considered by IEEE 802.16j is shown in Fig.1, where two kinds of radio links are identified: access link and relay link. BS that is capable of supporting multi-hop relay is called MR-BS. The access link is the radio link that originates or terminates at an MS, which is either a downlink (DL) or an uplink (UL), defined in IEEE 802.16-2004. The relay link is the radio link between an MR-BS and an RS or between a pair of RSs, which can be either uplink or downlink [68]. Based on the functionality of an RS, IEEE 802.16j has classified the RS functionality into two modes: transparent and non-transparent.

- In the transparent mode[62, 63], the RSs do not forward framing information, and hence do not increase the coverage area of the wireless access system; consequently, the main use case for

transparent mode relays is to facilitate capacity increases within the BS coverage area. This type of relay is of lower complexity, and only operates in a centralized scheduling mode and for topology up to two hops.

- In Non-transparent mode: The RSs generate their own framing information or forward those provided by the BS depending on the scheduling approach (i.e., distributed or centralized). They can support larger coverage areas and hence are mainly used to provide increased coverage. Fig.2 illustrates the two modes.

Table 1 below gives a comparison between the transparent and non-transparent relay modes [63, 64, 65].

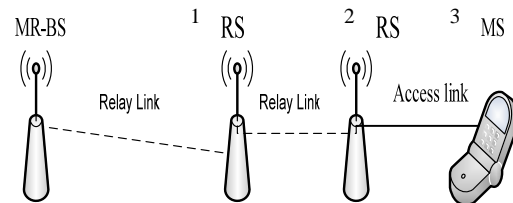


Fig.1 IEEE 802.16j basic system architecture

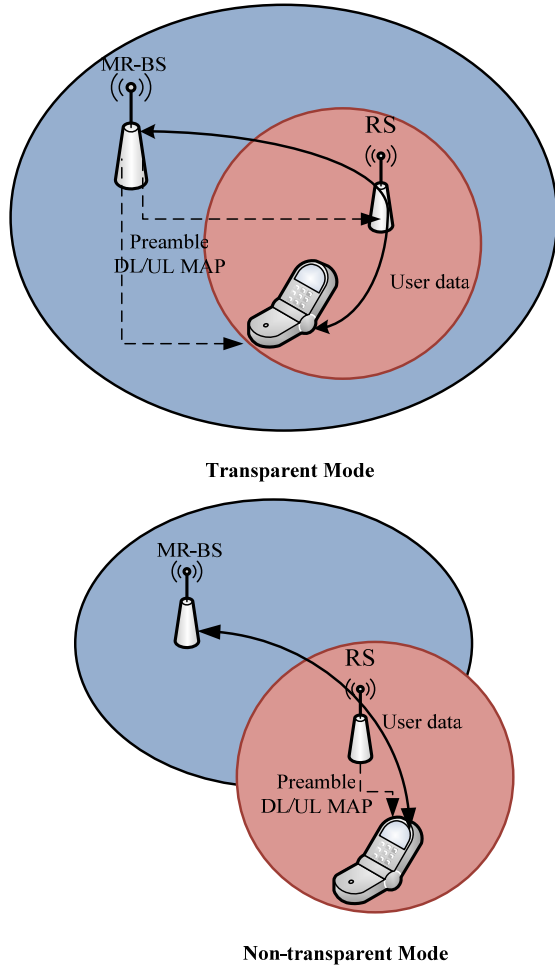


Fig.2 Transparent and Non-transparent relay modes architecture
Table 1: Transparent and Non-transparent relay modes

	<i>Transparent RS</i>	<i>Non-Transparent RS</i>
Coverage extension	No	Yes
Number of hops	2	> 2
Inter RS cell interference	NA	High
HO between RSs	None	Yes
Performance	In BS coverage: High Outer BS coverage: -	In BS coverage: same as 16e Outer BS coverage: medium
RS Cost	Low	High
Scheduling	Centralized only	Centralized/ distributed

There are two types of non-transparent relays available in 802.16j: Time-division Transmit and Receive (TTR) relay and Simultaneously Transmit and Receive (STR) relay. The TTR relay act in the access zone as BS and in relay zone it acts as relay.

For this work, we have considered the non-transparent mode with two TTR relays nodes.

2.2 Frame structure for MMR

As the frame structure defined in the earlier

IEEE 802.16e standards was designed for single-hop wireless networks, modifications were required to support relay network architectures. The IEEE 802.16e have adopted orthogonal frequency-division multiple access (OFDMA) as the primary channel access mechanism for non-line-of-sight (NLOS) communications in the frequency bands below 11 GHz. The basic unit of resource for allocation in OFDMA is a slot, which comprises a number of symbols in time domain, and one subchannel in frequency domain. The base station divides the timeline into contiguous frames, each of which further consists of a downlink (DL) and an uplink (UL) subframe. For the case where MR-BS supports more than two-hop relay, the DL and UL sub-frames shall include at least one access zone and may include one or more relay zone to enable RS operating in either transmit or receive mode. The DL/UL access zones are dedicated for transmission between MSs and their access stations (MR-BS or RS), and they are fully compatible with the 802.16e frame structure. The DL/UL relay zones are dedicated for transmission between MR-BS and the RS or between two RS. In each relay zone, BS and RS can stay in the mode of transmission, reception or being idle. However, it is not expected to have BS or RS switch from one mode to the other within the same zone. In order to give wireless device sufficient time to switch from one mode to another, the corresponding time gap (e.g., TTG and RTG) is inserted between two consecutive sub-frames. The IEEE Std. 802.16j specifies the following gaps:

- R-TTG: RS transmit/receive transition gap between uplink access zone and uplink relay zone in RS frame
- R-RTG: RS receive/transmit transition gap between uplink access zone and uplink relay zone in RS frame.

The case where each DL and UL sub-frame comprises of more than one relay zones is shown in Fig. 3.

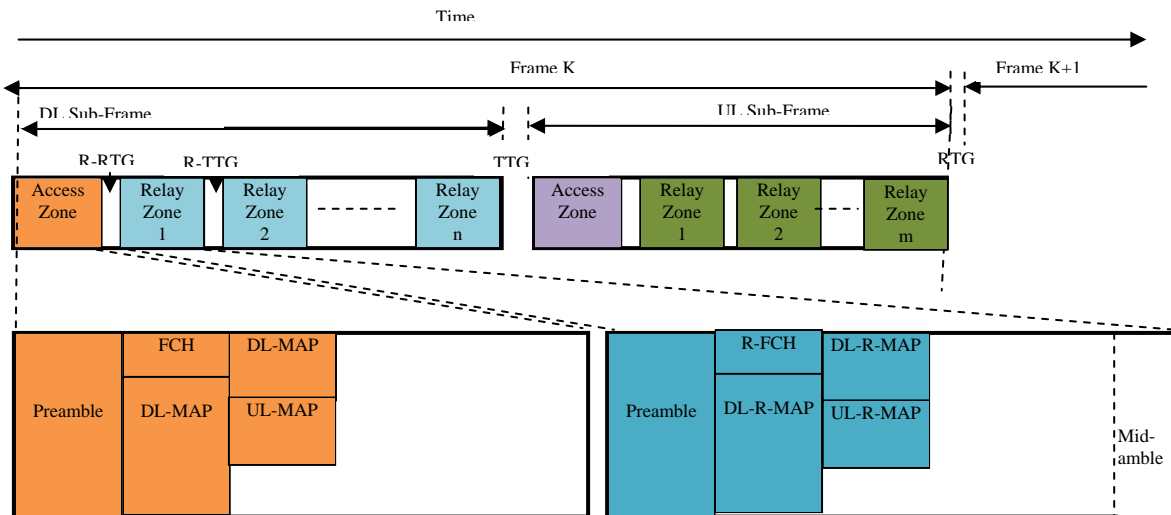


Fig.3 Frame Structure for MMR

The frame structure design is more challenging in the new mobile multihop relay based (MMR) network architecture, as numerous dimensions of design constraints and challenges have been introduced. In the literature frame structure design has received some attention In [48][49] a generic frame structure to support mobile multihop relay (MMR) operation of IEEE 802.16j, while maintaining the backward compatibility with the legacy 802.16e mobile stations was proposed and analyzed.

The packet construction mechanism in IEEE 802.16/16e standard, which was designed for handling traffic solely on a per-connection basis, cannot apply on the relay link directly, as it may render a potential bottleneck and preponderantly limit the overall network capacity. As a solution, in [58] the authors propose two schemes at the MAC layer, namely MPDU concatenation and MSDU aggregation.

3 Frame structure for MMR in non transparent mode with tunneling and network coding approach

This section provides design frame structure for multi relay hops (MR-BS, RS1, RS2) in non transparent mode. The proposed design takes in consideration network coding approach between relays. An envisioned topology is illustrated in figure 1, wherein RSs help MR-BS communicate with those MSs that are either too far away from the MR-BS. In other hand RSs can also have their own traffic to MSs. In this case, both the MR-BS and the relay transmit control data at the beginning of the frame. This way, the MS can synchronize with the relay, which is synchronized with the MR-BS.

The main drawback in the non-transparent case is that now the relay and BS are transmitting simultaneously in

time and possibly, frequency. The immediate drawback is an increase in interference, particularly in the preamble and control channels. Clearly, power control and frequency reuse, which largely are left up to manufacturers, are crucial to non-transparent relaying. Further, non-transparent relays likely are more sophisticated (and thus, more expensive) than transparent.

Therefore, our challenge is to design a transmission mechanism suitable for wireless multi-hop networks, which linearly combine information flows from (BS, RS1, RS2) into one flow to transmit.

The IEEE 802.16j is also devoted to defining a new MAC message family (called R-MAC) between the MRBS and the subordinate RSs. A fundamental part of the R-MAC is what can be regarded as a tunnel connection, which is identified by a special tunnel CID (T-CID). In what way to use these tunnels is not specified in 802.16j D2 [59]. In this work we take in consideration Hop by Hop Tunnel Establishing (HHTE). In HHTE, RS_i receives the MPDU from MS, MR-BS or RS_j, decodes it, and determines that it needs to be processed by each hop. RS_i encapsulates the MPDUs and sends it. Although the tunneling is optional, tunneling simplify the relaying process in multi-hop environment.

In order to explain our approach, we consider the topology illustrated by figure 1 which corresponds to 3 hops non transparent mode. We try to address the division of an IEEE 802.16j frame into different zones. We suggest the frame structure shown in fig.4 to support 3 hops non transparent TTR mode. We consider that MR-BS has the data flow X₀ to transmit to MS3 and each relay node RS_i has a data flow denoted X_i to be transmitted to the MS3. Moreover, the MS3 terminal has the data flows Y₀ and Y_i to send respectively to MR-BS and RS_i. The different interval time are denoted (T1, T2, T3, T4, T5, T6).

In table 2 we illustrate the data flows assigned and exchanged between the different hops.

Table 2: Data flow for support 3 hops non transparent mode

T1	T2	T3	T4	T5	T6
RS2 → MS3	MR-BS → RS1	RS1 → RS2 RS1 → MR-BS	MS3 → RS2	RS2 → RS1	RS1 → RS2 RS1 → MR-BS
X2k, X1(k-1), X0(k-1)	X0k	(X0k xor Y0(k-1)), (X1k)	Y2k, Y1(k), Y0(k)	Y0(k), Y1(k)	(Y0k xor X0k), (X1k)

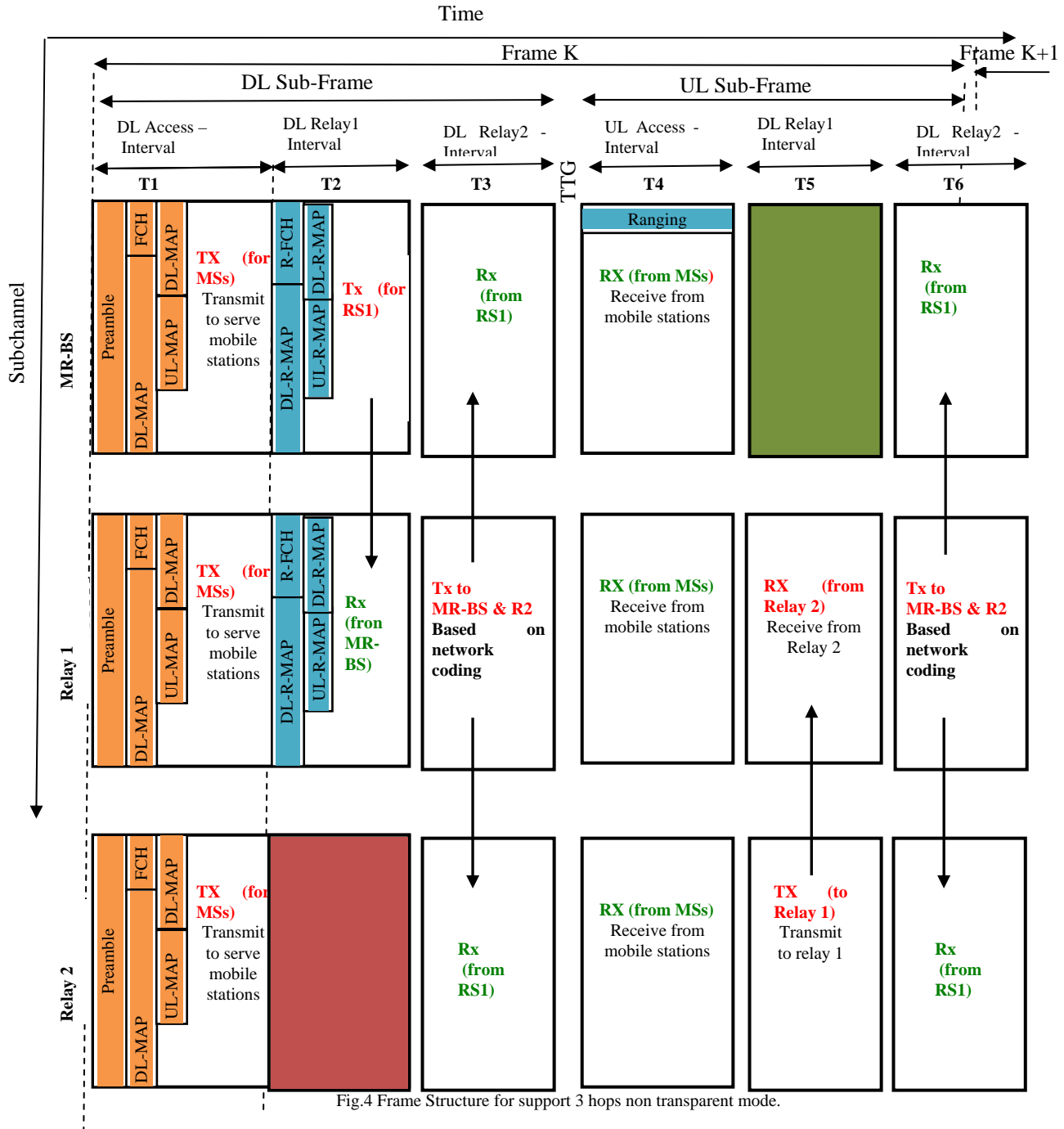


Fig.4 Frame Structure for support 3 hops non transparent mode.

In order to enhance the reliability of the wireless link, retransmission protocols have been widely adopted in

wireless systems. Usually, they assume that lost packets within a cell have to be retransmitted from the corresponding BS based on the ARQ protocol. In this case, The MR-BS receives twice the data flow Y_{0k} (in frame_k and frame_(k+1)) and the RS2 receives twice the data flow X_{0k} (in T3 and T6) this is can avoid the repeated retransmissions performed by the BS that reduce latencies to receive packets correctly.

4 Conclusions

In this paper, we have presented a coded cooperative networking MAC protocol in non transparent multihop WiMax. The proposed solution takes in consideration network coding approach between relays. The suggested frame structure supports 3 hops non transparent TTR mode.

In IEEE 802.16 based multi-hop networks many issues are still open both in PHY and MAC layer and specially those taken in consideration cross layer interaction. Key issues such as multi-hop frame structure, scheduling mechanism, support for QoS and many other requirements are under consideration. In future work, we will consider more extensive simulation to compare our scheme with other schemes.

References

- [1] Andrea Conti, Jiangzhou Wang, Hyundong Shin, Ramesh Annavajjala, and Moe Z. Win, "Wireless Cooperative Networks", EURASIP Journal on Applied Signal Processing, special issue published in volume 2008, 142 pages.
- [2] Anna Scaglione, Dennis L. Goeckel and J. Nicholas Laneman, "Cooperative Communications in Mobile Ad-Hoc Networks: Rethinking the Link Abstraction", book chapter in Distributed Antenna Systems: Open Architecture for Future Wireless Communications, edited by Honglin Hu, Yan Zhang, Jijun Luo, June 2006, © Taylor and Francis Group
- [3] Ramesh Chembil Palat, "Performance Analysis of Cooperative Communication for Wireless Networks, thesis, Faculty of Virginia Polytechnic Institute and State University, December 8, 2006, 164 pages.
- [4] Maric, I.; Yates, R.D, "Cooperative multihop broadcast for wireless networks" , Selected Areas in Communications, IEEE Journal on, Volume 22, Issue 6, Aug. 2004 Page(s): 1080 - 1088
- [5] J. Nicholas Laneman, COOPERATIVE DIVERSITY Models, Algorithms, and Architectures, Book chapter: Cooperation in Wireless Networks: Principles and Applications. Springer, 2006, pp. 163-188.
- [6] John Boyer, "Cooperative Connectivity Models and Bounds for Wireless Relay Networks", thesis, Ottawa-Carleton Institute for Electrical and Computer Engineering Department of Systems and Computer Engineering Carleton University, Ottawa, Ontario, Canada, 2007, 258 pages.
- [7] Suhas Mathur, Lalitha Sankar, Narayan B. Mandayam, Coalitions in Cooperative Wireless Networks, IEEE JOURNAL

ON SELECTED AREAS IN COMMUNICATIONS, VOL. 26, NO. 7, SEPTEMBER 2008.

[8] Ivana Maric, Roy Yates, "Static and Dynamic Cooperative Multicast for Maximum Network Lifetime", Allerton Conference on Communications, Control and Computing, Monticello, IL, Sept. 2004.

[9] Simone Frattasi, "Link Layer Techniques Enabling Cooperation in Fourth Generation (4G) Wireless Networks, thesis, International Doctoral School of Technology and Science Aalborg University, 26 September 2007

[10] Furuzan Atay, "Cooperative Diversity Relaying Techniques in Wireless Communication Networks", thesis, Faculty of Graduate Studies and Research, The Ottawa-Carleton Institute for Electrical and Computer Engineering (OCIECE) Department of Systems and Computer Engineering, January 2009, 199 pages.

[11] Chris T. K. Ng, J. Nicholas Laneman, Andrea J. Goldsmith, "The Role of SNR in Achieving MIMO Rates in Cooperative Systems, Information Theory Workshop ITW '06 Punta del Este, Uruguay, 13-17 March 2006, page(s): 288-292, ISBN: 1-4244-0035-X.

[12] Abbas El Gamal, "Capacity Theorems for Relay Channels", Department of Electrical Engineering, Stanford University, April, 2006

[13] Ivana Marié, Andrea Goldsmith, Gerhard Kramer and Shlomo Shamai Shitz, "On the capacity of interference channels with one cooperating transmitter", EUROPEAN TRANSACTIONS ON TELECOMMUNICATIONS, 2008; 19:405-420 Published online 24 April 2008 in Wiley InterScience.

[14] Katti, Sachin Maric, Ivana Goldsmith, Andrea Katabi, Dina Medard, Muriel MIT, "Joint Relaying and Network Coding in Wireless Networks", Information Theory, 2007. ISIT 2007. IEEE International Symposium , Nice, 24-29 June 2007, page(s): 1101-1105, ISBN: 978-1-4244-1397-3.

[15] Stefan Valentin, Hermann S. Lichte, Holger Karl, Guillaume Vivier, Sébastien Simoens Josep Vidal and Adrian Agustin, "Cooperative wireless networking beyond store-and-forward: Perspectives in PHY and MAC design", Wireless Personal Communications, Vol. 48, No. 1, pp. 49-68, Jan. 2009.

[16] S. Valentin, H. S. Lichte, H. Karl, I. Aad, L. Loyola, and J. Widmer, "Opportunistic relaying vs. selective cooperation: Analyzing the occurrence-conditioned outage capacity," in Proc. 11th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), Oct. 2008.

[17] Luo, J. Blum, R.S. Cimini, L.J. Greenstein, L.J. Haimovich, A.M., "Decode-and-forward cooperative diversity with power allocation in wireless networks" , IEEE Global Telecommunications Conference, GLOBECOM '05, Dec. 2005, Louis, MO St, Volume: ISBN: 0-7803-9414-3.

[18] Sadek, A.K.; Weifeng Su; Liu, K.J.R., "Performance analysis for multi-node decode- and-forward relaying in cooperative wireless networks", IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP 2005) , 18-23 March 2005, Volume 3, Issue , 18-23 March 2005.

[19] YINDI JING AND HAMID JAFARKHANI, " Beamforming in Wireless Relay Networks", Information Theory and Applications Workshop, Jan 2008, page(s): 142-150, ISBN: 978-1-4244-2670-6.

[20] Simoens, S. Vidal, J. Munoz, O. , "Compress-And-Forward Cooperative Relaying in MIMO-OFDM Systems", IEEE 7 th workshop: Signal Processing Advances in Wireless

Communications, SPAWC '06. , 2-5 July 2006, Cannes, page(s): 1-5, ISBN: 0-7803-9711-8.

[21] Ivana Maric, Roy D. Yates, Gerhard Kramer, "The Strong Interference Channel with Unidirectional Cooperation", in Proc. Information Theory and Applications (ITA), Inaugural Workshop, Feb. 2006.

[22] Furuzan Atay Onat, Yijia Fan, Halim Yanikomeroglu, H. Vincent Poor, "Threshold Based Relay Selection in Cooperative Wireless Networks", Global Telecommunications Conference, IEEE GLOBECOM Dec 2008. pages 1-5, ISSN: 1930-529X, ISBN: 978-1-4244-2324-8.

[23] Yindi Jing Jafarkhani, H., "Single and Multiple Relay Selection Schemes and their Diversity Orders", Communications Workshops, May 2008. ICC Workshops '08. Beijing, page(s): 349-353, ISBN: 978-1-4244-252-0.

[24] Y. Jing and H. Jafarkhani, "Single and Multiple Relay Selection Schemes and Their Achievable Diversity Orders," to appear in IEEE Transactions on Wireless Communications.

[25] J. Nicholas Laneman, David N. C. Tse, Gregory W. Wornell, "Cooperative Diversity in Wireless Networks: Efficient Protocols and Outage Behavior", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 50, NO. 12, DECEMBER 2004, 19 pages.

[26] Jose Lopez Vicario, Albert Bel, Antoni Morell and Gonzalo Seco-Granados, "Outage Probability vs. Fairness Trade-off in Opportunistic Relay Selection with Outdated CSI", EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING. Accepted 20 January 2009.

[27] Hunter, T. E. and A. Nosratinia: 2002, 'Cooperation diversity through coding'. In: Proc. IEEE Int. Symposium on Information Theory (ISIT). p. 220.

[28] Todd E. Hunter, Aria Nosratinia, "Diversity through Coded Cooperation", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 5, NO. 2, FEBRUARY 2006, pages 283→ 289.

[29] Yackoski, J.; Lu Zhang; Bo Gui; Chien-Chung Shen; Cimini, L.J., "Realistic Evaluation of Cooperative Relaying Networks Using Decentralized Distributed Space-Time Block Coding", Communications Workshops ICC, IEEE International Conference, 19-23 May 2008.

[30] J. Nicholas Laneman, , and Gregory W. Wornell, "Distributed Space-Time-Coded Protocols for Exploiting Cooperative Diversity in Wireless Networks", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 49, NO. 10, OCTOBER 2003, page(s) 2415→ 2426.

[31] Zhixin Liu; Stankovic, V.; Zixiang Xiong, "Wyner-Ziv coding for the half-duplex relay channel", IEEE International Conference on Acoustics, Speech, and Signal Processing, (ICASSP apos;05), Volume 5, Issue , 18-23 March 2005, Page(s): v/1113 - v/1116.

[32] Nadia Fawaz, David Gesbert and Merouane Debbah, "When Network Coding and Dirty Paper Coding meet in a Cooperative Ad Hoc Network", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, 2008, 6 pages.

[33] Ajay Gopinathan, Zongpeng Li, "Optimal Layered Multicast with Network Coding: Mathematical Model and Empirical Studies", 16th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS 2008), Baltimore, Maryland, USA, September 8-10, 2008. IEEE Computer Society 2008, ISBN 978-1-4244-2818-2 , page(s) 71-80.

[34] Yalin Evren Sagduyu, Anthony Ephremides, "ON NETWORK CODING FOR STABLE MULTICAST COMMUNICATION", Military Communications Conference, MILCOM 2007. IEEE Volume , Issue , 29-31 Oct. 2007.

[35] Andrea Munari, Francesco Rossetto, Michele Zorzi, "On the viability of a Cooperative-Network Coding Protocol in Clustered Networks", Military Communications Conference, 2008. MILCOM Nov 2008. IEEE

[36] Dereje H. Woldegebreal Stefan Valentin, Holger Karl, "Outage Probability Analysis of Cooperative Transmission Protocols without and with Network Coding: Inter-User Channels based Comparison", International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems Chania, Crete Island, Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems , Greece , 2007, Pages: 36 – 44, ISBN:978-1-59593-851-0.

[37] 802.16™ IEEE Standard , "Local and metropolitan area networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems", 3 Park Avenue, New York, NY 10016-5997, USA, IEEE Computer Society and the IEEE Microwave Theory and Techniques Society Sponsored by the LAN/MAN Standards Committee, October 2004, Print: SH95246, PDF: SS95246.

[38] IEEE 802.16 Working Group Officers, " 802.16j-06/026r3, Baseline Document for Draft Standard for Local and Metropolitan Area Networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Multihop Relay Specification, 2007-04-10.

[39] IEEE 802.16m-08/003, the Draft IEEE 802.16m System Description Document, 2008-01-23.

[40] Su Yi, Babak Azimi-Sadjadi, Shivkumar Kalyanaraman, Vijayanarayanan Subramanian, "Error Control Code Combining Techniques in Cluster-based Cooperative Wireless Networks", IEEE International Conference on Communications, 16-20 May 2005, Vol 5, On page(s): 3510- 3514, ISBN: 0-7803-8938-7.

[41] Stefan Valentin, Tobias Volkhausen, Furuzan Atay Onat, Halim Yanikomeroglu, and Holger Karl, "Decoding-based channel estimation for selective cooperation diversity protocols", IEEE 19th International Symposium: Personal, Indoor and Mobile Radio Communications, PIMRC, Cannes, France Sept 2008. Page(s): 1-6, ISBN: 978-1-4244-2643-0.

[42] Lu Zhang and Leonard J. Cimini Jr., "Power-Efficient Relay Selection in Cooperative Networks Using Decentralized Distributed Space-Time Block Coding", Hindawi Publishing Corporation, EURASIP Journal on Advances in Signal Processing, Volume 2008.

[43] Aggelos Bletsas, Ashish Khisti, David P. Reed, "A simple cooperative diversity method based on network path selection", IEEE Journal Selected Areas Communication Vol 3, March 2006.

[44] Zongpeng Li and Baochun Li, "Improving Throughput in Multihop Wireless Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 55, NO. 3, MAY 2006.

[45] Stefan Valentin, Holger Karl, "Effect of user mobility in coded cooperative systems with joint partner and cooperation level selection", In Proc. of IEEE Wireless Communications and Networking Conference (WCNC), March 2007.

[46] Lu Zhang and Leonard J. Cimini, Jr., "Hop-by-Hop Routing Strategy for Multihop Decode-and-Forward Cooperative Networks", IEEE Wireless Communications and Networking Conference, WCNC, April 2008.

[47] Deqiang Chen, Kambiz Azarian, and J. Nicholas Laneman, "A Case For Amplify-Forward Relaying in the Block-Fading Multi-Access Channel", IEEE Transactions on Information Theory 54(8), (2008).

- [48] Koon Hoo Teo, Zhifeng Tao and Jinyuan Zhang, Anfei Li, "Adaptive Frame Structure for Mobile Multihop Relay (MMR) Network", Information, Communications & Signal Processing, 2007 6th International Conference on Volume , Issue , 10-13 Dec. 2007 Page(s):1 - 5
- [49] Tao, Z.; Li, A.; Teo, K.H.; Zhang, J., "Frame Structure Design for IEEE 802.16j Mobile Multihop Relay (MMR) Networks", IEEE Global Telecommunications Conference (GLOBECOM), ISBN: 978-1-4244-1043-9, pp. 4301-4306, November 2007
- [50] Giuseppe Caire, Nihar Jindal, Mari Kobayashi., Gif-sur-Yvette, « Multiuser MIMO Downlink Made Practical: Achievable Rates with Simple Channel State Estimation and Feedback Schemes », Submitted to IEEE Trans. Information Theory, Nov. 2007, 46 pages.
- [51] Helmut Bolcskei, Rohit U. Nabar, Ozgur Oyman, "Capacity Scaling Laws in MIMO Relay Networks", IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 5, NO. 6, JUNE 2006, page(s) 1433-1445.
- [52] Yalin Evren Sagduyu, Anthony Ephremides, "A Game-Theoretic Look at Simple Relay Channel", ACM/Kluwer Journal of Wireless Networks, vol. 12, no. 5, pp. 545-560, Oct. 2006.
- [53] J. Nicholas Laneman, "Cooperative Diversity in Wireless Networks: Algorithms and Architectures", Thesis in Electrical Engineering at the MASSACHUSETTS INSTITUTE OF TECHNOLOGY, September 2002
- [54] John Boyer, David D. Falconer, Halim Yanikomeroglu, "Cooperative Connectivity Models for Wireless Relay Networks", Wireless Communications, IEEE Transactions on Volume 6, Issue 6, June 2007 Page(s):1992 - 2000
- [55] Hermann S. Lichte and Stefan Valentin, "Implementing MAC Protocols for Cooperative Relaying: A Compiler Communications, Networks and Systems (SIMUTools), Mar. 2008, Best paper award.
- [56] Yalin Evren Sagduyu, "MEDIUM ACCESS CONTROL AND NETWORK CODING FOR WIRELESS INFORMATION FLOWS", Thesis, 2007, Department of Electrical and Computer Engineering.
- [57] Pei Liu, Zhifeng Tao, Sathya Narayanan, Thanasis Korakis, and Shivendra S. Panwar, "CoopMAC: A Cooperative MAC for Wireless LANs", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 25, NO. 2, FEBRUARY 2007.
- [58] Tao, Z.; Teo, K.H.; Zhang, J., "Aggregation and Concatenation in IEEE 802.16j Mobile Multihop Relay (MMR) Networks", IEEE Mobile WiMAX Symposium, pp. 85-90, March 2007
- [59] Junkai Zhang Suili Feng1 We Ye Hongcheng Zhuang, MAC Performance Evaluation of IEEE 802.16j, 2008 International Symposium on Information Science and Engineering.
- [60] Peters, S.W.; Heath, R.W.; The future of WiMAX: Multihop relaying with IEEE 802.16j, Communications Magazine, IEEE Volume 47, Issue 1, January 2009 Page(s):104 - 111
- [61] Basak Can, Halim Yanikomeroglu, Furuzan Atay Onat, Elisabeth De Carvalho and Hiroyuki Yomo, "Efficient Cooperative Diversity Schemes and Radio Resource Allocation for IEEE 802.16j", IEEE Wireless Communications and Networking Conference, WCNC , March 31 2008-April 3 2008, page(s): 36-41, ISSN: 1525-3511, ISBN: 978-1-4244-1997-5
- [62] Vasken Genc, Sean Murphy, John Murphy, "Analysis of Transparent Mode IEEE 802.16j System Performance with Varying Numbers of Relays and Associated Transmit Power", IEEE Communications & networking conference , IEEE WCNC, 5-8 April 2009 , Budapest Hungary.
- [63] Vasken Genc, Seán Murphy, John Murphy, "Performance Analysis of Transparent Relays in 802.16j MMR Networks", IEEE 6th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops, WiOPT, 1-3 April 2008, page(s): 273-281, ISBN: 978-963-9799-18-9.
- [64] VASKEN GENC, SEAN MURPHY, YANG YU, AND JOHN MURPHY, "IEEE 802.16J RELAY-BASED WIRELESS ACCESS NETWORKS: AN OVERVIEW", IEEE Wireless Communications • October 2008.
- [65] Masato okuda, Chenxi zhu, Dorin viorel, "Multihop relay extension for wimax networks – An overview and benefits of IEEE 802.16j standard", FUJITSU SCIENTIFIC & TECHNICAL JOURNAL FSTJ, Special Issue 1: Fujitsu's Mobile WiMAX Solutions, 2008-4 Vol.44, No.3.
- [66] Mike Hart & Jung Je Son, "Harmonized definitions and terminology for 802.16j Mobile Multihop Relay", IEEE 802.16 Broadband Wireless Access Working Group, IEEE 802.16j-06/014r1.

First Author Dr Lamia CHAARI was born in Sfax, Tunisia, in 1972. She received the engineering and PhD degrees in electrical and electronic engineering from Sfax national engineering school (ENIS) in TUNISIA. Actually she is an assistant professor in multimedia and informatics higher institute in SFAX She is also a researcher in electronic and technology information laboratory (LETI). Her scope of research are communications, networking and signal processing which are specially related to wireless and new generation networks.

Second Author Pr Lotfi Kamoun was born in Sfax Tunisia, 25 January. 1957. He received the electrical engineering degree from the Sciences and Techniques Faculty in Tunisia. Actually he is a Professor in Sfax national engineering school (ENIS) in TUNISIA. He is the director of electronic and technology information laboratory (LETI). His scope of research are communications, networking, Software radio and signal processing which are specially related to wireless and new generation networks.

Authentication and Secure Communication in GSM, GPRS, and UMTS Using Asymmetric Cryptography

Wilayat Khan¹ and Habib Ullah²

¹ Department of Electrical Engineering, COMSATS Institute of IT,
Wah Cantt, 47040, Pakistan

² Department of Electrical Engineering, COMSATS Institute of IT,
Wah Cantt, 47040, Pakistan

Abstract

With its great features like providing access to users at anytime and anywhere in the world, mobile communication has been very attractive among the users as well as operators and service providers. However, despite of several advantages, mobile communication has also been facing many security problems. In 2G and 3G technologies like GSM, GPRS and UMTS, the architectures comprise of mainly three nodes; the mobile station (MS), Visitor Location Register/Serving GPRS Support Node (VLR/SGSN), and Home Location Register /Authentication Center (HLR/AuC). These nodes are involved to encrypt/decrypt the data and authenticate the user (MS) in GSM, GPRS and UMTS. To provide security services like authentication and secure communication, the mechanism has been moved from symmetric cryptography to, despite of its complexity, asymmetric cryptography. To reduce the signaling overhead and add some other security features, we propose a new generalized approach in this paper. This is based on asymmetric cryptography for user/network authentication and communication encryption in GSM/GPRS and UMTS with reduced signaling overhead.

Keywords: GSM, GPRS, UMTS, Authentication, Security, Asymmetric Key Cryptography.

1. Introduction

Wireless and mobile communication systems are very famous among the customers as well the operators and service providers. Unlike wired networks, the wireless networks provide anywhere and anytime access to users. The *Global System for Mobile Communications* (GSM) occupy almost 70% of the wireless market and is used by millions of subscribers in the world [1].

In the wireless services, secure and secret communication is desirable. It is the interest of both, the customers and the

service providers. These parties would never want their resources and services to be used by unauthorized users.

The services like online banking, e-payment, and e/m-commerce are already using the Internet. The financial institutions like banks and other organizations would like their customers to use online services through mobile devices keeping the wireless transaction as secure as possible from the security threats. Smart cards (e.g. SIM card) have been proposed for applications like secure access to services in GSM to authenticate users and secure payment in Visa and MasterCard [2]. Wireless transactions are facing several security challenges. Wireless data passing through air interface face almost the same security threats as the wired data. However, the limited wireless bandwidth, battery, computational power and memory of wireless devices add further limitations to the security mechanisms implementation [3].

The use of mobile communication in e/m-commerce has increased the importance of security. An efficient wireless communication infrastructure is required in every organization for secure voice/data communication and users authentication. Among the main objectives of an efficient infrastructure is to reduce the signaling overhead and reduce the number of updating *Home Location Register/Authentication Center* (HLR/AuC) while the *Mobile Station* (MS) changes its location frequently [3].

In this paper, we propose an approach based on public key cryptography which mainly focuses on user and network authentication with reduced signaling overhead and meet other security requirements like non-repudiations, safety from denial-of-service attacks and integrity of authentication signaling messages.

The rest of the paper is organized as follows. Section 2 gives a brief overview of GSM systems architecture and section 3 discusses authentication protocol used in GSM/GPRS. Section 4 describes authentication and communication encryption in UTM. Some related work is discussed in section 5. In section 6, we propose a new approach for user and network authentication and communication encryption. Finally, after short discussion, a conclusion is drawn.

2. GSM Overview

GSM, the *Group Special Mobile*, was a group formed by *European Conference of Post and Telecommunication Administrations* (CEPT) in 1982 to develop cellular systems for the replacement of already incompatible cellular systems in Europe. Later in 1991, when the GSM started services, its meaning was changed to *Global System for Mobile Communications* (GSM) [1].

The entire architecture of the GSM is divided into three subsystems: *Mobile Station* (MS), *Base Station Subsystem* (BSS) and *Network Subsystem* (NSS) as shown in Figure 1. The MS consists of *Mobile Equipment* (ME) (e.g. mobile phone) and *Subscriber Identity Module* (SIM) which stores secret information like *International Mobile Subscriber Identity* (IMSI), secret key (Ki) for authentication and other user related information (e.g. *certificates*).

The BSS, the radio network, controls the radio link and provides a radio interface for the rest of the network. It consists of two types of nodes: *Base Station Controller* (BSC) and *Base Station* (BS). The BS covers a specific geographical area (hexagon) which is called a *cell*. Each cell comprises of many mobile stations. A BSC controls several base stations by managing their radio resources. The BSC is connected to *Mobile services Switching Center* (MSC) in the third part of the network NSS also called the *Core Network* (CN). In addition to MSC, the NSS consists of several other databases like *Visitor Location Register* (VLR), *HLR* and *Gateway MSC* (GMSC) which connects the GSM network to *Public Switched Telephone Network* (PSTN). The MSC, in cooperation with HLR and VLR, provides numerous functions including registration, authentication, location updating, handovers and call routing. The HLR holds administrative information of subscribers registered in the GSM network with its current location. Similarly, the VLR contains only the needed administrative information of subscribers currently located/moved to its area. The *Equipment Identity Register* (EIR) and *AuC* contains list of valid mobile equipments and subscribers' authentication information respectively [1, 5].

3. Authentication and Ciphering in GSM and GPRS

There are various security threats to networks [6]. Among these threats are *Masquerading or ID Spoofing* where the attacker presents himself as to be an authorized one, unauthorized use of resources, unauthorized disclosure and flow of information, unauthorized alteration of resources and information, repudiation of actions, and *denial-of-service*. The GSM network incorporates certain security services for operators as well as for their subscribers. It verifies subscribers' identity, keeps it secret, keeps data and signaling messages confidential and identifies the mobile equipments through their *International Mobile Equipment Identity* (IMEI). In the next subsections, we explain subscribers' authentication and data confidentiality as they are closely related to our topic [5].

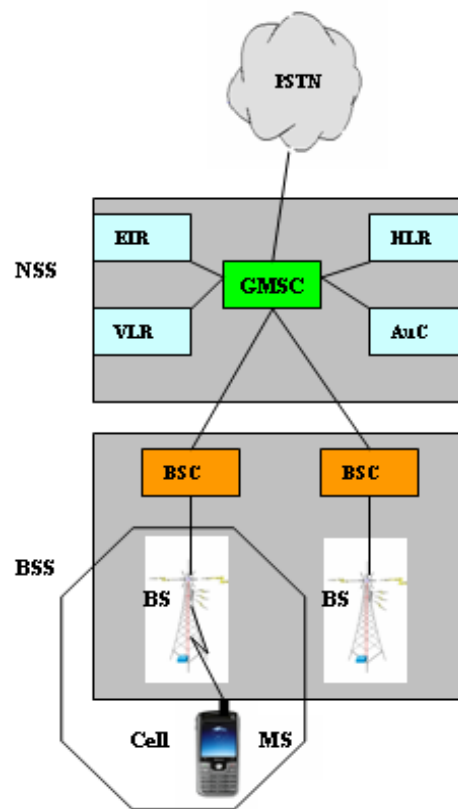


Figure 1. Components overview of GSM

3.1 Subscribers Identity Authentication

As mentioned above, the SIM card holds IMSI, phone number, authentication key K_i , subscriber-relevant data and security algorithms like authentication algorithm (A3). The HLR also stores a copy of K_i and IMSI etc.

In GSM, the users are first identified and authenticated then the services are granted. The GSM authentication protocol consists of a challenge-response mechanism. The authentication is based on a secret key K_i which is shared between HLR and MS. After a visited MS gets a free channel by requesting BS, it makes a request for its location update to MSC through BSC. The MSC, in response, asks MS for its authentication.

In the entire authentication process, the three main actors are the MS, MSC/VLR and HLR/AuC as given in Figure 2. The mobile station sends its *Temporary Mobile Subscriber Identity* (TMSI) to VLR in its request for authentication. The MS uses its real identity IMSI when it is switched on for the first time but the temporary identity TMSI is used later. The TMSI is used to provide *anonymity* to the user identity. After getting the IMSI of the mobile station from the old VLR using TMSI, the VLR sends IMSI to the corresponding HLR/AuC. The HLR/AuC uses authentication algorithm (A3) and ciphering key generation algorithm (A8) to create the encryption key (K_c) and *Signed RESult* (SRES) respectively.

The HLR sends the triplet including K_c , RAND and SRES to VLR. The VLR sends the RAND challenge to MS and ask to generate an SRES and send it back. The mobile station creates an encryption key K_c and SRES using algorithms A3 and A8 with the inputs secret key K_i and RAND challenge. It stores K_c to use it for encryption and sends SRES back to the VLR. The VLR compares SRES with the one sent by HLR. If they match, the authentication succeeds otherwise it fails [1, 4, 5].

3.2 User Data and Signaling Protection

The encryption key K_c is used by both of the parties (home system and mobile station) to encrypt the data and signaling information using A5 algorithm. The encryption is done by mobile equipment not the SIM because SIM does not have enough power and processing capacity [1, 4, 5].

4. Authentication and Ciphering in UMTS

The UMTS, in fact, is the result of evolution in GSM network through GPRS. The GSM networks are capable of voice communication using *Circuit Switched* (CS) technique while GPRS adds *Packet Switched* (PS) technique through the use of some extra nodes like *Serving GPRS Support Node* (SGSN) and *Gateway GPRS Support Node* (GGSN). The UMTS, incorporating GPRS nodes and *UMTS Terrestrial Radio Access Network* (UTRAN), provides both circuit switched and packet switched services with enhanced multimedia applications.

As stated in 3GPP specification [7], the circuit switched services are provided by VLR and the packet switched services are provided by SGSN. The UMTS, like GSM/GPRS, uses the concept of *Authentication Vector* (AV) but unlike GSM/GPRS, the AV comprises of five components: the random challenge (RAND), the expected response (XRES), key for encryption (CK), integrity key (IK) and the authentication token (AUTN). The VLR/SGSN requests HLR/AuC for authentication. The HLR/AuC computes the AV and is sent back as a response to VLR/SGSN without any encryption applied to it. After the authentication is completed, the cipher key CK is used to encrypt the user data and signaling information. Similarly, to preserve the integrity of the important control signals, integrity key (IK) is used.

The GSM Consortium actually provided security to GSM systems relying on *security through obscurity* where they believed that the algorithms used in GSM would be very hard to break if they were kept secret. Therefore, the GSM specifications and protocols were kept secret away from public to be studied and analyzed by scientific community.

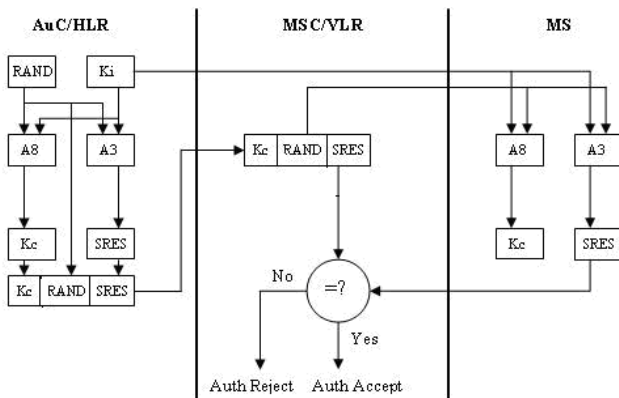


Figure 2. The GSM authentication architecture

But, eventually, the GSM algorithms were accessed by scientific community and now GSM is vulnerable to many attacks [6, 7, 10].

In GSM/GPRS and UMTS, the links between MS-VLR and VLR-HLR faces many security threats due the use of conventional symmetric key encryption and mutual trust of the parties. The VLR and HLR just rely on mutual trust they have on each other.

To implement public key cryptography, a well defined network infrastructure is needed. The *Public Land Mobile Network* (PLMN) operators are the main candidates for this to develop PKI in their systems. The 3G networks like UMTS which offers services with very high data rates is the most favorable for the operators to incorporate PKI services to their customers. To verify the authenticity of public keys, there should be a trusted third party, the *Certification Authority* (CA), to issue digital certificates to the users. These certificates are to be stored in the SIM/USIM of the mobile station. The *Mobile Execution Environment* (MExE) is an application execution environment which allows application programming and creating a *Java Virtual Machine* (JVM) in the MS. Based on the importance of secure transactions and the fact that networks operators are the big candidates for PKI implementation, it seems feasible to use public-private key pair for intra-PLMN signaling as well as for secure e/m-transaction. A new approach, with the introduction of asymmetric key cryptography, has been adopted in [8].

5. Related Work

Asymmetric key approach supported by MExE is another reason to be favorable for operators to deploy *Public Key Infrastructure* (PKI) in their systems. The asymmetric key cryptography for authentication and encryption, as mentioned in [8], is described below.

5.1 Asymmetric Cryptography in GSM/GPRS and UMTS

As in GSM/GPRS, we consider the same three nodes: MS, VLR and HLR/AuC. These nodes preserve the same roles for all the three systems: GSM, GPRS and UMTS, involved in the process of authentication and encryption.

The nodes VLR and HLR hold the same pair of public-private keys, $V_{H_{PrK}}$ and $V_{H_{PuK}}$, which facilitates the key distribution process because other interconnected networks would need only one public key for corresponding VLR-HLR transactions. A second option could be to use separate public-private key pairs but it will further complicate the key distribution process. The link

between VLR and HLR is secured using the VLR-HLR public key ($V_{H_{PuK}}$). The messages are encoded with this key by any of the endpoints. At the receiving end, the corresponding private key $V_{H_{PrK}}$ is used for decryption.

After the channels are assigned, the users are authenticated through the exchange of messages among the nodes: MS, VLR and HLR as shown in Figure 3. The MS (SIM on mobile station) sends an *Identity Message* to VLR which includes the identity data (e.g. IMSI of the user) encrypted with MS-VLR's public key ($MS_{V_{PuK}}$). The VLR decodes it using corresponding private key ($MS_{V_{PrK}}$) and extracts the required information. The VLR encrypts it again with VLR-HLR link public key ($V_{H_{PuK}}$) and forwards it to the corresponding HLR in *Authentication Information* message. After it is decoded using VLR-HLR link private key ($V_{H_{PrK}}$), the HLR sends the user's public key (MS_{PuK}) back to the VLR in an *Authentication Acknowledgment* message. The VLR sends a random challenge *RAND* to the MS encrypted with the user's public key (MS_{PuK}) in *Authentication Request* message. The MS decodes the random number, encrypts it with its own private key and sends it back along with SK and IK to VLR in *Authentication Response* message. The VLR decrypts this message using the user's public key and checks if the random number is the same. If it is equal to the random number held by VLR, it will indicate the user authenticity as it has been signed by the user with his own private key.

Public key cryptography is computationally extensive. Therefore, it slows down the data rate. It can be better utilized when it is used for secret keys transmission. The SIM on the MS creates *secret key* (SK) and in case of

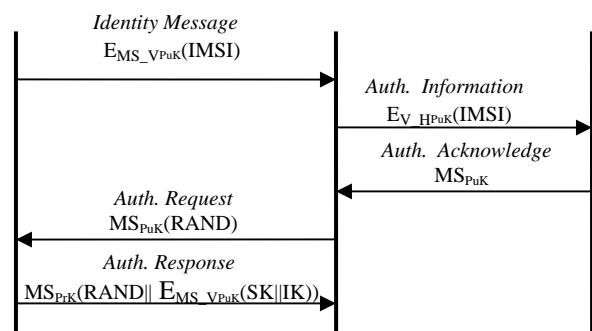


Figure 3. Authentication process using public key cryptography

UMTS an *integrity key* (IK) for the integrity of signaling messages. These two keys are concatenated, encrypted with VLR's public key ($MS_{V_{PuK}}$) and are sent to the VLR in the *Authentication Response* message. After the authentication is successful, the data and signaling information are encrypted with the keys SK and IK to preserve the confidentiality and integrity of both the data and signals.

The public key cryptographic approach discussed in the above paragraphs is an obvious way of authentication and securing the communication especially when it is used in financial transactions like e/m-commerce. In this approach, five messages are exchanged to authenticate the user and to share the keys which brings signaling overhead. In this approach, the user (MS) is authenticated by the network before giving the service but it does not authenticate the network. One can rely only on the fact that both, the MS and the HLR, have the same secret key Ki. This can be considered a weak network authentication, but it will fail if the key Ki is stolen or accessed by a third party. The *denial-of-service* attack is possible if the attacker changes the authentication signaling (signal integrity). In the next section, we propose a general solution with reduced signaling for all the three systems GSM, GPRS and UMTS to reduce the drawbacks discussed above.

6. Authentication and Encryption in GSM, GPRS and UMTS Using Public Key Cryptography

Due to slow data rates, the public key encryption offers, it is not encouraged to be used for communication encryption. Instead, it is preferred for authentication and secret key distribution to be used in symmetric key encryption of the communication. To encrypt the data and signaling, special secret and integrity keys like SK and IK may be used respectively for communication encryption and signaling integrity.

In this section, we present a solution based on public key cryptography. This relies on the same concept of public-private keys as mentioned in the section 5. The three main entities, MS, VLR and HLR, are using four pairs of public-private keys as shown in Figure 4(a).

These three entities exchange four messages with each other as shown in Figure 4(b). The detail of the elements in each of these messages is

$$\begin{aligned} \text{Identity Message} &= E_{M_{V_{PuK}}} (IK||SK||RAND) || E_{H_{PuK}} (IMSI||Ki) \\ \text{Authentication Information} &= E_{H_{PuK}} (IMS||Ki) \end{aligned}$$

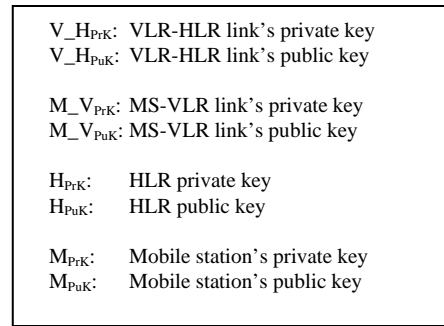


Figure 4(a). Set of public keys used

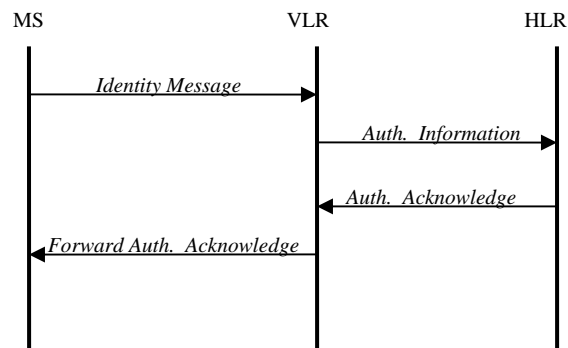


Figure 4(b). Authentication process using public key cryptography

$$\begin{aligned} \text{Authentication Acknowledge} &= M_{PuK} \\ \text{Forward Authentication Acknowledge} &= E_{M_{PuK}} (RAND) \end{aligned}$$

The symbol ‘||’ represents the concatenation of two elements. The MS creates secret keys SK, IK and a random challenge RAND. It starts the authentication exchange by sending an *Identity Message* to the visited VLR. This message includes concatenation of RAND, SK and IK encrypted with public key $M_{V_{PuK}}$. The IMSI and Ki encrypted with public key H_{PuK} is also part of the *Identity Message* as shown in Figure 4(b). Unlike the approach in [8], the secret keys SK and IK are sent in the first message.

The VLR uses the corresponding private key $M_{V_{PrK}}$ to decode the part of the message and extract the needed information RAND, SK and IK. The VLR forwards the rest of message ($E_{H_{PuK}}(IMS||Ki)$) unchanged in *Authentication Information* message to the HLR. The keys

SK and IK are used later for confidentiality and integrity of both the data and signals respectively.

The HLR decodes the *Authentication Information* message with its private key H_{PrK} and gets the IMSI and Ki sent from MS. The secret key Ki is used as a random challenge for user/MS authentication. The MS and the HLR have the same secret key Ki. The HLR compares the received Ki with its own Ki. If they match, the user is authenticated. It is difficult for a third party to change this secret without being detected by HLR. The HLR can easily detect it using IMSI of the requesting user sent in the *Identity Message*.

Using the IMSI, the HLR finds the corresponding user's public key M_{PuK} and is sent to VLR in the *Authentication Acknowledge* message. This message acts as an indication to the VLR that the user has been authenticated by the HLR. The VLR uses the public key M_{PuK} to encrypt the RAND challenge received from MS in the *Identity Message*. The MS decrypts it with its own private key. The result is compared with the RAND stored at MS. If they are equal, the VLR is authenticated as it ensures the MS that the VLR is the only entity having the MS-VLR link's private key M_{VPrK} .

This approach includes all the benefits of the previous systems. It keeps the user's identity secret, the encryption keys are distributed, users and network both are authenticated. This entire process requires four signaling messages reducing the signaling overhead.

An attack *denial-of-service* may be possible if the attacker changes the signaling contents based on which the user and network authenticates each other. For example, if the encrypted content of RAND challenge is modified or if IMSI or Ki is changed during transmission, the network and user authentication will fail even if the user and network are legitimate. To cope with this problem, *Digital Signature* [9] can be used. The end-to-end integrity of the authentication parameters should be ensured because the end entities, the VLR/HLR and the MS, make the decision of authentication. Therefore, to ensure the integrity of message contents at the ends, *hashing* (H) function combined with encryption may also be used. For example the elements IMSI and KI may be hashed using the secret key Ki and the resulted message digest is sent in the *Identity Message*. This will ensure the HLR that the parameters IMSI and Ki have not been altered during transmission.

7. Conclusions

Wireless communication, having great features, is attractive among users as well service providers. With the increase in its use, security problems of confidentiality, integrity, and authentication are also increasing. The mechanism to solve these problems has changed to public key cryptography from symmetric key cryptography. The available public key cryptographic approaches are good in security point of view but they are computationally extensive as well as have more signaling overhead. Furthermore, these approaches do not provide integrity of the initial authentication messages and authentication of the network.

In this paper, we proposed an enhanced model based on the public key cryptography. In this model, utilizing the real benefits of public key encryption, user as well as network authentication is provided. The integrity of the signaling used during the user and network authentication is ensured. The secret keys for data encryption and signaling integrity are distributed using public keys. These benefits are achieved with fewer signals reducing the signaling overhead.

As noted before, although, public key cryptography is computationally very extensive which requires large processing power, battery, and memory, but still the approach we proposed is efficient to use than the others. The rapid developments in *Integrated Circuits* (IC) and *Smart Cards* (e.g. SIM) technologies, high speed communication systems (e.g. UMTS), and significance of secure transactions (e.g. e/m-commerce) make the conditions more favorable to use public key cryptography.

References

- [1] Yong Li, Yin Chen, and Tie-Jun MA, "Security in GSM", Retrieved March 18, 2008, from <http://www.gsm-security.net/gsm-security-papers.shtml>.
- [2] N. T. Trask and M. V. Meyerstein, "Smart Cards in Electronic Commerce", A SpringerLink journal on *BT Technology*, Vol. 17, No. 3, 2004, pp. 57-66.
- [3] N T Trask and S A Jaweed, "Adapting Public Key Infrastructures to the Mobile Environment", A SpringerLink journal on *BT Technology*, Vol. 19, No. 3, 2004, pp. 76-80.
- [4] Cheng-Chi Lee, Min-Shiang Hwang, and I-En Liao, "A New Authentication Protocol Based on Pointer Forwarding for Mobile Communications", A Wiley InterScience journal on *Wireless Communications and Mobile Computing*, Published online, 2007.
- [5] Vesna Hassler and Pedrick Moore, "Security Fundamentals for E-Commerce", Artech House London Inc., 2001, pp. 356-367.
- [6] Mohammad Ghulam Rahman and Hideki Imai, "Security in Wireless Communication", A SpringerLink journal on

Wireless Personal Communications, Vol. 22, No. 2, 2004, pp. 213-228.

- [7] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Mobile Execution Environment (MExE); Service Description, Stage I. Technical Specification 3G TS 22.057 version 5.2.0 (2001-10), 2001.

Wilayat Khan graduated with a B.Sc. in Computer Systems Engineering from the NWFP University of Engineering & Technology, Pakistan in 2007. He earned his MS degree from the Royal Institute of Technology (KTH) Sweden in Information and Communication Systems Security in 2009. In his MS theses, he designed a strong authentication protocol for handheld devices. In 2009, he started his carrier as a teacher at the Department of Electrical Engineering, COMSATS Institute of IT, Wah Campus, Pakistan. He has published a number of papers on wireless and mobile networks and security in international journals and conference proceedings. His research interests include wireless & mobile networks, protocol design for mobile devices, authentication, web security and smart cards security.

Habib Ullah graduated in B.Sc. Computer Systems Engineering from the NWFP University of Engineering & Technology, Pakistan in 2006 and earned M.Sc. degree in Electronics and Computer Engineering from the Hanyang University, Seoul Korea with a thesis focusing on comparative study: the evaluation of shadow detection methods. He started teaching in 2009 at the department of Electrical Engineering, COMSATS Institute of IT, Wah Campus, Pakistan. He has various publications focusing on background modeling and shadow detection. His research interests include information security, pattern recognition, behavior modeling and object segmentation etc.

Touching Syllable Segmentation using Split Profile Algorithm

L.Pratap Reddy¹, T.Ranga Babu², N.Venkata Rao³ and B.Raveendra Babu⁴

¹ Department of Electronics and Communication Engineering,
JNTUH College of Engineering, Hyderabad - 500085, Andhra Pradesh, India

² Department of Electronics and Communication Engineering,
RVR & JC College of Engineering, Guntur - 522019, Andhra Pradesh, India

³ Department of Electronics and Communication Engineering,
Sri Vasavi Engineering College, Tadepalligudem - 534101, Andhra Pradesh, India

⁴ Department of Computer Science and Engineering,
RVR & JC College of Engineering, Guntur - 522019, Andhra Pradesh, India

Abstract

The most challenging task of a character recognition system is associated with segmentation of individual components of the script with maximum efficiency. This process is relatively easy with regard to stroke based and standard scripts. Cursive scripts are more complex possessing a large number of overlapping and touching objects, where in the statistical behavior of the topological properties are to be studied extensively for achieving highest accuracy. Certain amount of similarity exists between unconstrained hand written text as well as South Indian scripts in terms of topology, component combinations, overlapping and merging characteristics. The concept of syllables and their formulations is an additive complexity with regard to Indian scripts. In this paper the statistical behavior of the cursive script, Telugu, is presented. The topological properties in terms of zones, component combinations, behavioural aspects of syllables are studied and adopted in the segmentation process. The statistical behaviour of cursive components are evaluated. Split Profile Algorithm is proposed while handling touching components. The proposed algorithm is evaluated on different fonts and sizes. The performance of the proposed algorithm is compared with two approaches methods viz aspect ratio and syllable width approaches.

Keywords: Segmentation, Connected Components, Syllable Segmentation, Touching Syllable, Split Profile Algorithm.

1. Introduction

Document image analysis and Optical Character Recognition (OCR) systems are under continuous research for decades. The transformation of paper media into the searchable and revisable text format gives a great boost in

the field of language technology based research. Automated content creation from printed or written form of ancient and later versions of documents is the major area of OCR research. Achieving accurate results under all possible conditions remains as a challenging task. The first step in this process is to achieve maximum efficiency in character segmentation, which in turn reflects in OCR accuracy.

Script topology plays a dominant role in the segmentation process. Structural features describe the patterns of topology and geometry while exploring global and local properties. White spaces and pitch information are the useful primitive parametric data of any segmentation system. The notion of detecting vertical white space between successive characters is an important concept while dissecting images of machine print and even in hand written documents. Apart from this, other topological features like height, width and orientation etc., are useful parameters. In case of fixed width characters, pitch information provides effective segmentation. However, variable width characters are found in almost all scripts due to large number of font designers. As a result, various segmentation approaches are proposed [1] in literature to handle this complexity.

Structural properties of natural language script are another useful piece of information, to be adopted while choosing the segmentation approach. Scripts can be further classified as stroke based, cursive and hybrid. Segmentation of stroke based scripts can be performed by

making use of properties like horizontal, vertical and slant line information.

Segmentation approaches that are to be adopted for cursive scripts are complex when compared with stroke based scripts. Character shapes of these scripts possess variable widths and sizes, originated from a combination of more than one component. The topological or structural properties of individual components and their associative nature with other components transform the final shape, occasionally leading to overlapping and touching phenomena. Segmentation issues of these scripts are to be addressed by considering common statistical properties along with specificities of the respective class of formulations. On the other hand, hybrid model is associated with a set of strokes as well as curves. The primitive shape (glyph) is to be treated as the main focus of this model.

2. Review

Various segmentation methods adapted in document image processing are described [1] by Richard G. Casey and Eric Lecolinet. Profile based approach proposed [2] by K. Ohta which is considered as a simple and effective method for segmenting a print line. These approaches are reported to be effective for non-cursive writing systems and still found their applications even in handwritten recognition systems. Detection of white spaces can be effectively carried out on a structured text image. Identification and extraction of vertical strokes is made simple using this method. Analysis of peaks and valleys of profile patterns extended the scope of profile method for partial adaptation into touching character segmentation. In [1], the profile was first obtained and then the ratio of second derivative of this pattern to its height is used as a criterion for identifying segment separation. The peak of the derivative, which is associated with projection minima converge the splitting points along the thin horizontal lines.

A peak-to-valley function is proposed in [3] by Y. Lu with further improvements. Spatial domain characteristics based on the topological features of the script are explored. Valleys between successive peaks are extracted from the profile function. An average function is used to identify the extract segment point with a specific reference to touching characters. A selection criterion of the segmentation boundary is associated with discriminating function of topological features of individual characteristics.

Bounding box approach [4] is proposed by M. Cesar and R. Shinghal as an alternative to profiling method. They reported that the method is effective on stroke based script. Splitting and merging of character component is reported

in [4]. The connected component approach proposed in this work is mainly concentrated on defining specific rules using height and width parameters of bounding box. The adjacency relationships between bounding boxes, their size and aspect ratios are explored for splitting mechanisms. Segmentation effectiveness is reported with high degree of accuracies even at low computational requirements. Extension of connected component approaches is proposed in [5] by G. Seni and E. Cohen for segmentation of hand written words in a document image.

The CJK script models are more predominant in strokes and relationships among the strokes are well structured [6]. Latin text, European language models describe the dominance of strokes. The linear property of strokes is explored in using profile based approach while segmenting characters of all the above scripts.

North Indian scripts are hybrid in nature, combining strokes and curves, where strokes are dominated by curves. Linear spatial relationship in the form of shirorekha (a straight line combining components) can be found within the topological structure. The resultant form of this linear relation is treated as zone, which is used to establish correlation among strokes and curves within the syllables. The top zone of the character resembles stroke like geometry. The positional information of zone is identified by finding the linear region from the profile function of script line. Segmentation is achieved by exploring the statistical properties [7,8,9,10,14] of zone information using profile based methods.

Arabic and South Indian scripts are dominated by curve like components. In Arabic scripts, the formation of character is nonlinear and base line is identified by the peak of vertical profile function [11]. South Indian scripts are derived from the writing style on palm leaves, resembling cursive nature in machine print as well as hand written. The process of character formulations resulting from component combinations with zero width joiner and some times with non joiner leading to overlapping phenomena. Character formation in these scripts (also known as syllable) deals with two part glyphs in certain cases, deviating from the linear process. Notable number of non-linear combinations exists in these scripts. Segmentation is to be addressed by taking into consideration of all processes, linear and non-linear combinations. In this context, the statistical behavior of component shapes within the boundaries of text line, any word and even a syllable, influences the segmentation strategies.

In South Indian scripts, curves are more predominant and extraction of zone information is complex. Syllable is formed by a set of curves with high degree of similarity among them. The individual components in the syllable are

extracted and associated relationship is studied using zone information. The extraction of zone information is complex because of the non-linear distribution of glyphs in the upper and bottom regions. Common properties are reported in [12,13] by extensive statistical evaluation of the profile function.

Profile method [11] found its use not only in printed text but also in hand written text. Handwritten profile information of the script line is used to identify the linear portions of the script characters. The profile information of a word differs from that of a line. At the same time, multiple word combinations of a script line posses linear behavior in the profile patterns. Extensive statistical evaluation of various script lines is necessary while formulating rules in the zone identification process. Similar studies are extended to syllable segmentation in the present paper. A detailed description of segmentation model is presented in the following section.

3. Segmentation Model

The segmentation model in this paper explored the statistical patterns of profile vector which signifies the topology and geometry of printed text with specific reference to cursive script of Telugu. Preprocessing steps like binarisation, skew correction are carried out on the document image before proceeding to segmentation algorithm.

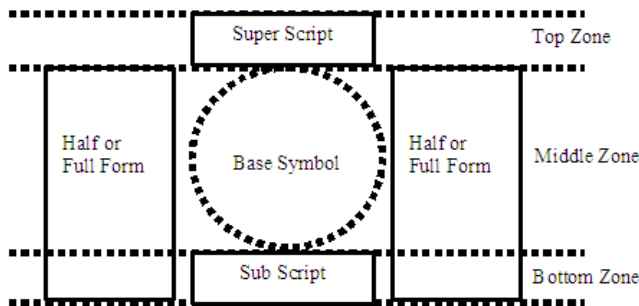


Fig. 1 Canonical Syllable Model.

Four phases are proposed in the segmentation process. First phase deals with line segmentation and extraction of zone information, second phase deals with syllable segmentation, third phase addressed the classification of segmented syllables into touching and non-touching objects and fourth phase is emphasised on segmentation of touching objects using Split Profile Algorithm (SPA).

In the first two phases, connected component approach is adopted for segmentation of syllable. Syllable model

proposed [13] by Pratap et al, presented in Fig. 1 and is adopted in the present phase.

Topology of the syllable can be decomposed into component like glyph objects. One base symbol object, also treated as essential component, is the minimum topology. In a complex conjunct syllable a maximum of four other components will be positioned, as in the above figure. The number of components may vary in between 1 and 5. However the topological features in the form of zones is difficult to extract due to the inherent nature of zero width joiner and non joiners between components. This phenomenon reflected in the form of touching syllables that are predominant in various font sizes.

Using the above model, syllable segmentation and classification of touching syllable is carried out in phase 2 and 3 respectively. In the last phase, segmentation of touching syllable is addressed with the help of SPA. Topology of various syllable components is studied after splitting the profile. Prediction of segmentation threshold is carried out in the separation process of touching syllables.

3.1 Line and Zone Separation

Different scripts posses varied structural features. However machine printed document images are structured in nature with a similarity around script line distribution. The linear property from pixel distribution of Horizontal projection Profile (HPP) is adopted for line segmentation. HPP is obtained using Eq.(1)

$$H_{PP}(i) = \sum_{j=1}^N f(i, j) \quad (1)$$

where $i = 1, 2, 3, \dots, M$ (Height of the object)
 $j = 1, 2, 3, \dots, N$ (Width of the object)

White spaces between text lines are treated as delimiters in ideal case. However under the influence of noise the profile distribution between lines reflects the random nature of noise information. In the present case, we considered ideal scenario, where the noise component is negligible. Starting point and ending point of script line is found with certain amount of black pixel distribution, using which the lines are segmented.

Pixel distribution of script line is studied on various document images. Certain amount of linear behavior is found in the form of peaks and valleys, reflecting the zone information. The geometry of individual syllable does not match with zones, which is also the case with certain words where as multiple combinations of words found to

be linear. One peak in the first half of profile distribution is observed. This peak matched with zone separation line between top and middle zones. However zone separation line between middle and bottom zone is reflected in the form of maximum slope in the later half of the profile formation.

The detailed algorithm for Line and Zone separation is listed below

- Step 1 Extract horizontal profile vector for the whole document image.
- Step 2 Divide the Lines profile vector which consists of starting and ending of the line in the image and mark them as top line and bottom line respectively.
- Step 3 Extract first line from the document image
- Step 4 Divide the script line profile vector into two halves along the length.
- Step 5 Find the row with peak value of black pixel density in the first half of the profile vector and mark it as Head Line.
- Step 6 Find the rows with peak values of black pixel density in the later half of the profile vector.
- Step 7 Find the slope of the valley from the row in Step 6 with respect to the successive row.
- Step 8 The row with the maximum slope of the valley is identified as the base Line.
- Step 9 Extract the Top-Middle-Bottom zones of the script line. Get the zone information for different script lines.

Original document image is presented in Fig.2 Segmentation of lines and extraction of zone information, as defined in steps 1-5, is presented in Fig.3 and Fig.4.

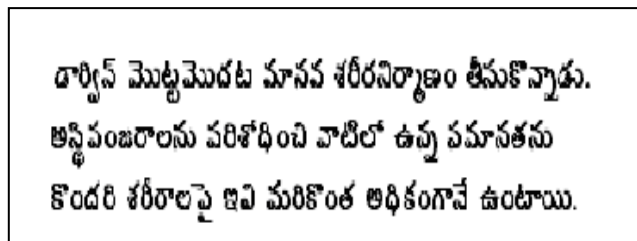


Fig. 2 Original Document Image.

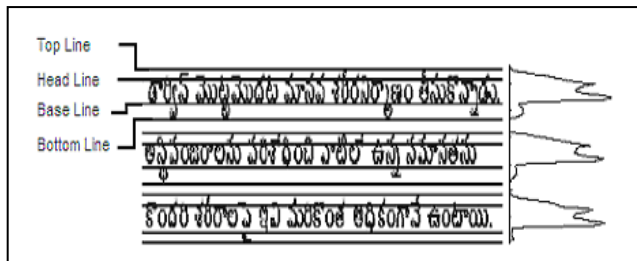


Fig. 3 Line & Zone separation fro horizontal profile.

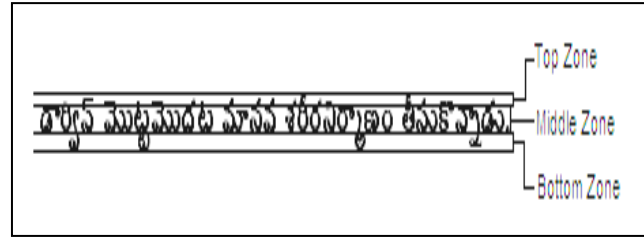


Fig. 4 Zone Information of text sample.

3.2 Syllable Segmentation

In an ideal scenario, individual glyph components (Fig.1) can be decomposed using zone information. The canonical space is extracted from the text document using connected component approach with a reported [13] segmentation efficiency of 95.72%, without addressing the touching syllables. Similar approach is adopted in the present phase. The component objects that are separable, are identified with the help of labeling approach. Grouping of core and non-core components are carried out while segmenting syllable objects. These objects may include touching syllables also. The syllable segmentation is given below

The detailed algorithm is as follows:

- Step 1 Extract the zone information for different script lines.
- Step 2 Label the pixels by scanning them from left to right in each row and row after row.
- Step 3 Find adjacent labels and connect the labels to form basic components.
- Step 4 Find unique labels and extract component with unique labels
- Step 5 Identify whether it is core component or non-core component using zone information
- Step 6 Merge the non-core components with core components using zone information.
- Step 7 Extract the Syllable from the input text image and draw the bounding box.

The concept of core component and other components in a syllable as proposed by Pratap Reddy et al. [13] is a reflective mechanism of the topology and geometry with regard to Telugu script. This property is explored in steps 1-7 and the result is presented in Fig.5.

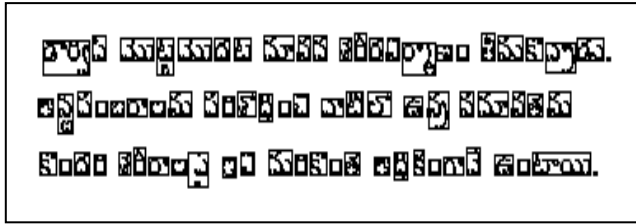


Fig. 5 Segmented Syllables of document image.

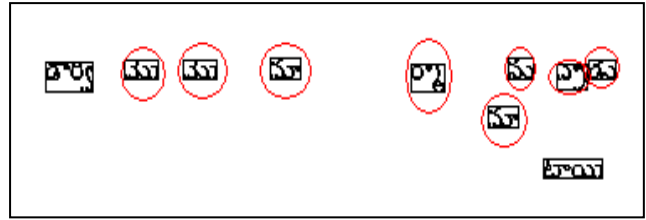


Fig. 7 Syllables classified as Touching syllable using Aspect Ratio

3.3 Classification of Correctly Segmented Syllables

In the process of improving segmentation efficiency, it is required to classify the correctly segmented syllables against the others. The syllable objects, extracted from the previous stage are a combination of touching and non-touching syllable objects. Aspect ratio (the relation between component height and width) is a simple approach adopted for this purpose which is defined in Eq.(2).

$$\text{Aspect Ratio}(A) = \frac{\text{Component Width}}{\text{Component Height}} \quad (2)$$

The optimum threshold Th_{ASP} is defined in Eq.(3)

$$Th_{ASP} = \left[\frac{\sum_{i=1}^N A(i)}{N} \right] \quad (3)$$

Th_{ASP} is an averaging function of the relationship between component objects, which is used as a threshold value. The syllable object with $A \geq Th_{ASP}$ is treated as touching syllable. Segmented output after adaptation of aspect ratio is presented in Fig.6 and Fig.7.

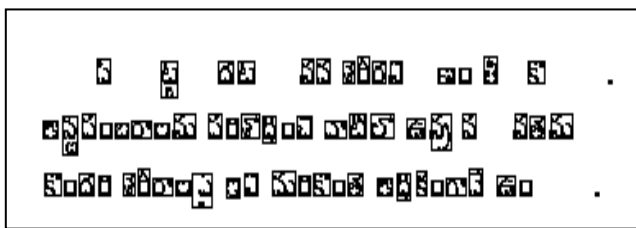


Fig. 6 Syllables classified as Single Syllable using Aspect Ratio.

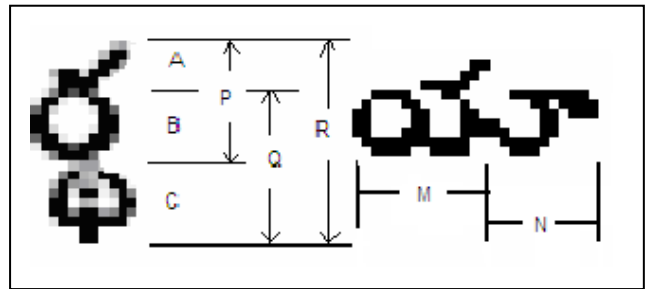


Fig. 8 Height and width variation of Syllable.

Topology of the script is so complex, at times height and width of a syllable posses large variations as described in Fig.8

The variables A,B,C define the height of top zone, middle zone and bottom zone layers. P,Q,R variables are computed as A+B, B+C, A+B+C respectively. It is quite interesting to see that the syllable height may have varying combination among B, P, Q, R. Similarly two different specifications can be made with regard to syllable width M, defined as core width and N, as modifier width. Two possibilities always exist. The width of the syllable may be M or some times extends to M + N depending on the type of modifiers. The value of M and N differs for each core component as well as modifiers. The possible combination of aspect ratio finally leads to 8 different types for each type of core component. There are 36 different types of core components, where the width and sizes differs slightly. In addition to that another 13 modifiers exists. The entire complexity can be visualised in the form of classification error leading to isolated syllables pushed into touching syllables. This error influences segmentation efficiency up to a large extent.

While resolving the segmentation problem and to reduce the classification error, it is necessary to identify effective classification mechanism. As per the evaluation in [15] the syllable groups and their frequency statistics reveal the fact that modifier combinations are only 16% of the text information. Large numbers of syllable groups are focused around core width. Average syllable width is one of the parameter for better judgment.

The optimum threshold for classification of syllable objects is redefined as Th_{SYW} (Average Syllable Width), and is given in Eq.4

$$Th_{SYW} = \left[\frac{\sum_{i=1}^N W(i)}{N} \right] \quad (4)$$

The outcome of the classifier using Th_{SYW} is presented in Fig.9 & Fig.10. It is observed that the error is now reduced further, while classifying touching syllable only.

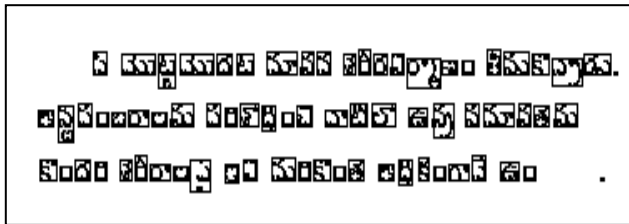


Fig. 9 Syllables classified as Single Syllable using Syllable Width.

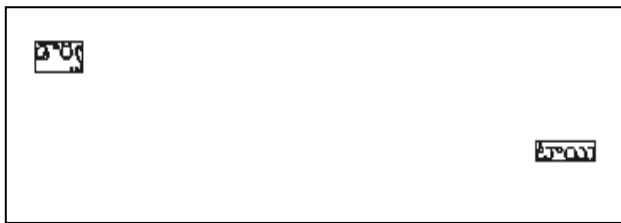


Fig. 10 Syllables classified as touching syllable using Syllable Width.

After careful analysis on 38,419 syllables (12,14,16 & 19 font sizes) of Anupama font, it is found that segmentation efficiency is 91.39% for Aspect ratio, where as 94.48% for Syllable width. An improvement of 3 % is observed. For Gowthami font (30,871 syllables) segmentation efficiency is observed as 86.63% and 89.20% for aspect ratio and syllable width respectively. In the case of Priyanka font average efficiency is observed as 81.73% and 87.32% respectively.

3.4 Split Profile Algorithm

The topology of the syllable, where cursive nature is more predominant, provides information about the placement and their relationship among the glyphs. The syllables are formed with the placement of glyph(s) with varying style and sizes. In certain occasions one syllable may overlap with the next syllable. This situation may appear at different zones of the syllable, resulting in complex behavior. The statistical analysis on different fonts

(Anupama, Gowthami and Priyanka) reveals the fact that large number of overlapped characters is present in small sized font structures. Some syllables with large width may be classified as touching syllable. They will play a major role on segmentation efficiency. Connected component approach fails in segmenting the touching characters for the reasons explained above.

To handle this problem we propose an alternative method, Split Profile Algorithm, where the profile information of the touching syllable will be split into two parts and the geometric features are studied for identification of touching labels.

Two parameters are introduced in the algorithm. The first one ‘Horizontal Split Threshold’ (ST_H) which is used to identify the splitting index of the text line segment. The second one ‘Vertical Split Threshold’ (ST_V), to identify the segment boundary of touching syllable.

Horizontal split threshold is defined as

$$ST_H = \text{Head Line} + ((\text{Bottom Line} - \text{Head Line})/2)$$

Vertical split threshold is defined as

$$ST_V = 2^{\text{nd}} \text{ transition point from low to high in the lower part of the profile}$$

Either the top segment or bottom segment can be considered for extraction of syllable index. The topology of the touching characters is mostly associated with positional structure of glyph like components. In this context one of the line segments will provide positional information of the above components. Vertical profile of the respective portions of line segments is plotted for this purpose. The profile part with multiple segments is used for defining segmentation index. From the statistical study it is observed that the starting point of the second component is the most likely predicted segment boundary from ST_V . The split profile algorithm which was applied is as follows

The algorithm for SPA

- Step 1 Get the horizontal profile of the syllable
- Step 2 Split the horizontal profile using ‘ ST_H ’
- Step 3 Get the vertical profile for the lower part of the image.
- Step 4 Split the touching syllable by using Vertical Split Threshold ‘ ST_V ’ index from the scaled profile obtained from step 3.

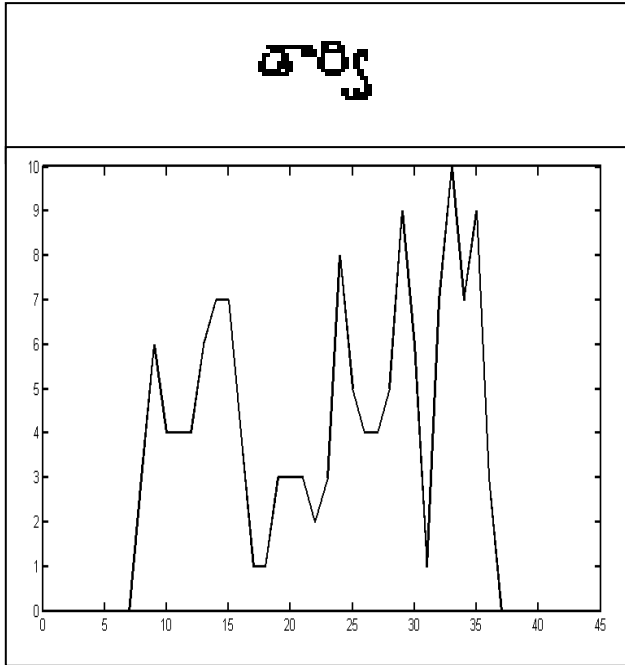


Fig. 11 Vertical Profile of the First Syllable

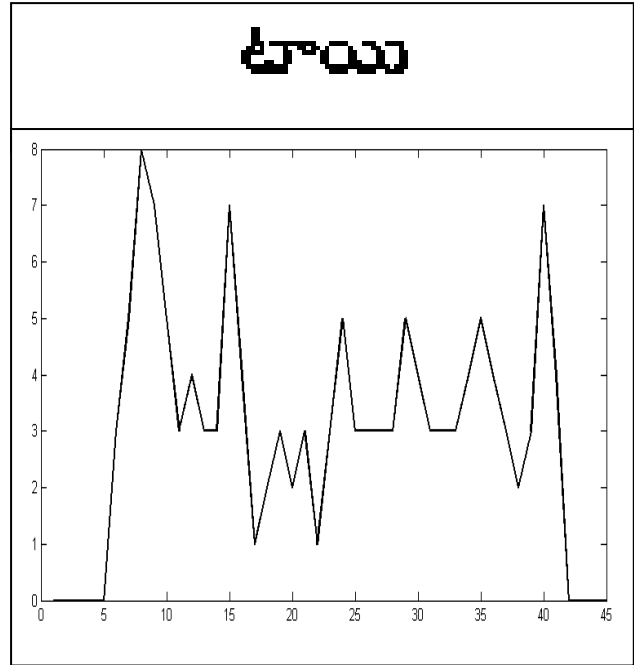


Fig. 13 Vertical Profile of the Second Syllable.

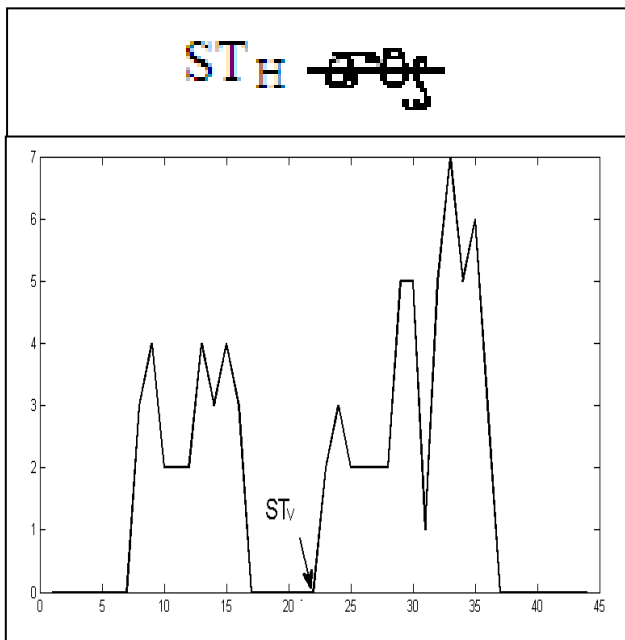


Fig. 12 Scaled Vertical Profile for the lower part of the First Syllable.

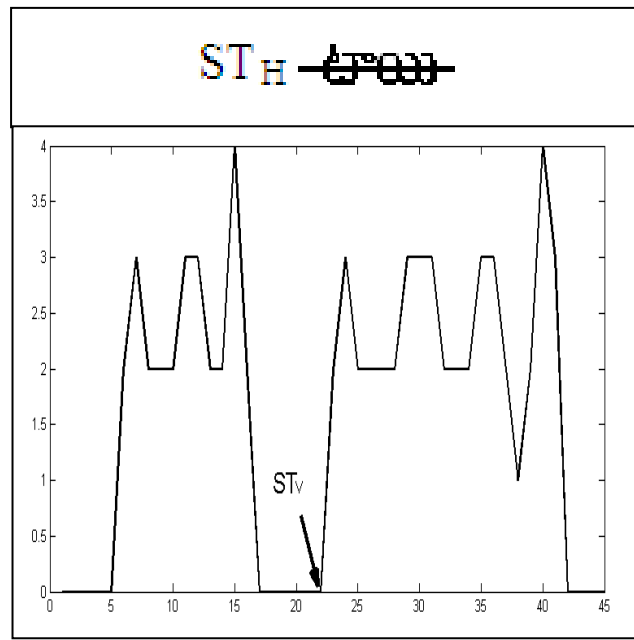


Figure 14. Scaled Vertical Profile for the lower part of the Second Syllable

Table 1: Output for the first syllable after SPA

అ	ం
---	---

Table 2: Output for the second syllable after SPA

ం	ం
---	---

4. Results

The proposed algorithm is evaluated on 1,11,582 syllables of Anupama, Gowthami, and Priyanka font. Segmentation is carried out on font sizes of 12,14,16 and 19. Syllable segmentation efficiencies of aspect ratio, syllable width and Split Profile Algorithm for Anupama font is presented in figures 15 to figures 18. SPA outperform with 100% segmentation efficiency on the sample set of size 14, 16 and 19. The syllable width based approach is observed with average segmentation efficiency of 98%. The aspect ratio based approach is observed with segmentation efficiency ranging from 97.93% to 98.04%. For font size 12, SPA is observed with maximum segmentation efficiency of 92.98% against 84.15% and 76.12% with syllable width and aspect ratio respectively. However, when evaluated on samples of font sizes 12,14,16 and 19, the average segmentation efficiency of SPA is observed as 92.98%, 100%, 99.96% and 100% where as syllable width approach is observed as 84.15%, 98.65%, 98.77% and 98.98% and aspect ratio is found to be 76.12%, 97.93%, 97.63% and 98.04% respectively. Comparison of segmentation efficiencies for different fonts and sizes presented in Table 3, 4 and 5

Table 3: Aspect Ratio

Font Size	12	14	16	19
Font Type	Segmentation efficiency			
Anupama	76.12	97.93	97.63	98.04
Gowthami	73.75	95.00	92.95	95.42
Priyanka	50.44	85.13	97.72	98.98

Table 4: Syllable Width

Font Size	12	14	16	19
Font Type	Segmentation efficiency			
Anupama	84.15	98.65	98.77	98.98
Gowthami	76.89	97.01	96.68	97.14
Priyanka	62.21	91.41	98.61	99.52

Table 5: Split Profile Algorithm

Font Size	12	14	16	19
Font Type	Segmentation efficiency			
Anupama	92.98	100.00	99.96	100.00
Gowthami	88.95	99.77	99.26	99.40
Priyanka	76.68	97.55	99.67	99.96

5. Conclusions

Topology and geometry is observed to be one of the important information of any script. Extensive study of the statistical properties with regard to topology is crucial while improving segmentation accuracy. In this paper an attempt is made towards this direction on popular cursive script Telugu. Profile function is considered for separating the linear region over non linear portions in the script line as well as touching syllables. A general approach (connected component approach) on these scripts is compared with the proposed Split Profile Algorithm. The highest performance of average segmentation efficiency with SPA is observed as 99.98%, 99.47% and 99.05% on ANUPAMA, GOWTHAMI and PRIYANKA fonts respectively. Experimental evaluation of the proposed algorithm on small font sizes is in progress. Extension of the proposed algorithm at the level of segmentation and classification with a priori knowledge is in progress.

References

- [1] Richard G. Casey and Eric Lecolinet, "A survey of methods and strategies in character segmentation" IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 18, No. 7, pp. 690-706, July 1996.
- [2] K. Ohta, I. Kaneko, Y. Itamoto, and Y. Nishijima, "Character Segmentation of Address Reading/Letter Sorting Machine" for the Ministry of Posts and Telecommunications of Japan, NEC Research and Development, vol. 34, no. 2, pp. 248-256, Apr. 1993
- [3] Y. Lu, "On the Segmentation of Touching Characters," Int'l Conf. Document Analysis and Recognition, Tsukuba, Japan, pp. 440-443, Oct. 1993.
- [4] M. Cesar and R. Shinghal, "Algorithm for Segmenting Handwritten Postal Codes," Int'l J. Man Machine Studies, vol. 33, no. 1, pp. 63-80, July 1990.
- [5] G. Seni and E. Cohen, "External Word Segmentation of Off-Line Handwritten Text Lines," Pattern Recognition, vol. 27, no. 1, pp. 41-52, Jan. 1994.
- [6] K.W. Gan, K.T. Lua, "A new approach to stroke and feature point extraction in Chinese character recognition". Pattern Recognition Letters, Vol. 12, no. 6, pp 381-386, June 1991

- [7] B. B. Chaudhuri, U. Pal, "A complete printed Bangla OCR system" Pattern Recognition, vol.31, No. 5, pp. 531- 549, March 1998.
- [8] Veena Bansal, R. M. K. Sinha, "Integrating knowledge sources in Devanagari text recognition system", IEEE Transactions on Systems, Man, and Cybernetics, Part A : Systems and Human, vol. 30, no. 4, pp 500-505, July 2000.
- [9] M. K. Jindal, G. S. Lehal, R. K. Sharma, "A Study of Touching Characters in degraded Gurmukhi Script", World Academy of Science, Engineering and Technology, vol.4, pp 121-124, 2005
- [10] U. Pal and Sagarika Datta, "Segmentation of Bangla Unconstrained Handwritten Text", Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR 2003), August 2003.
- [11] Liana M. Lorigo, Venu Govindaraju, "Offline Arabic Handwriting Recognition: A Survey" IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 28, no. 5, pp. 712-724, May 2006
- [12] Pratap Reddy L, Satyaprasad L, ASCS Sastry, "Middle Zone Component Extraction and Recognition of Telugu Document Image", Ninth International Conference on Document Analysis and Recognition, (ICDAR 2007), Vol 2, pp 584 – 588, September 2007.
- [13] Pratap Reddy, L. Sastry, A.S.C. Rao, A.V.S. Venkat Rao, N., "Canonical syllable segmentation of Telugu document images", TENCON 2008 - IEEE Region 10 Conference , pp 1-5, Nov-2008.
- [14] M. K. Jindal, R. K. Sharma, G. S. Lehal "Segmentation of touching characters in upper zone in printed Gurmukhi script", ACM Annual Bangalore Compute Conference, Article No.: 9, 2009 .
- [15] L. Pratap Reddy, "A New Scheme for Information Interchange in Telugu through Computer Networks", Ph.D. thesis, Department Electronics and Communication, JNTU University, Hyderabad, INDIA, May 2001.



L. Pratap Reddy received his B.E degree in Electronics and Communication Engineering from Andhra University, India in 1985, M.Tech. degree in Electronic Instrumentation from Regional Engineering College, Warangal, India in 1988 and Ph.D. degree from Jawaharlal Nehru Technological University, Hyderabad, India in 2001. From 1988 to 1990 he was lecturer in Department of

Electronics and Communication Engineering at Bangalore Institute of Technology, Bangalore, India, from 1991 to 2005 he was faculty member at JNTU College of Engineering, Kakinada, India. Since 2006 he is with Department of Electronics and Communication Engineering and presently he is Professor and Head of the department at JNTUH College of Engineering, Hyderabad, India. His current activity in research and development includes, apart from telecommunication engineering subjects, Image Processing, Pattern Recognition and Linguistic processing of Telugu language. He published more than 50 research publications in various National, Inter National conferences and Journals. He is active member in professional bodies like ISTE, IE, IETE, and CSI.



T. Ranga Babu received his B.E. degree in Electronics and Communication Engineering from University of Madras, India in 1992,

M.S. degree in Electronics & Control Engineering from Birla Institute of Technology and Science, Pilani, India in 1999 and M.Tech. degree in Electronics and Communication Engineering with specialization in Digital Electronics and Communication Systems from Jawaharlal Nehru Technological University College of Engineering (Autonomous), Anantapur, India in 2004. From 1992 to 2003 he was worked as faculty member in the Department of Electronics and Communication Engineering at different educational institutions and from 2003 he is working as Assistant Professor in the Department of Electronics and Communication Engineering at R.V.R & J.C. College of Engineering, Guntur, India. Currently he is working in the area of Image Processing, Natural Language Processing, Pattern Recognition and pursuing his Ph.D. in Jawaharlal Nehru Technological University Hyderabad, India. He is a Life member of ISTE, IETE, CSI and IACSIT.

N. Venkata Rao received his B.E degree in Electronics and Communication Engineering from Bangalore University, India in



1985 and M.Tech. degree in Electronics and Communication Engineering with specialization in Instrumentation and Control Systems from Jawaharlal Nehru Technological University, Kakinada, India in . He has 22 years of teaching experience as Assistant Professor, Associate Professor, Professor and he is currently working as Professor in the Department of Electronics and Communication Engineering, Sri Vasavi

Engineering College, Tadepalligudem, India. He has published 7 research papers in various National, Inter National conferences. Currently he is working in the area of Natural Language Processing, Image Processing, Pattern Recognition and pursuing his Ph.D. He is a Life member of ISTE and IETE.



B. Raveendra Babu received his M.S degree in Software Systems from Birla Institute of Technology and Science, Pilani, IN 1997, M.Tech degree in Computer Science and Engineering from Anna University, Chennai IN 2000, Ph.D degree from S.V. University, India in 1992. He has 26 years of teaching experience as Assistant Professor, Associate Professor, Professor and he is currently heading the

Department of Computer Science and Engineering at RVR & JC College of Engineering, Guntur, India. He is presently Chairman, Board of studies for Computer Science and Engineering, Acharya Nagarjuna University, India. He has published more than 20 research publications in various National, Inter National conferences, proceedings and Journals. His research areas of interest include VLDB, Image Processing, Pattern analysis and Wavelets. He is a life member for ISTE and CSI, member for ACM and IEEE Computer society.

Information Security and Sender's Rights Protection through Embedded Public Key Signature

Vineeta Khemchandani¹, Prof G.N.Purohit²

¹ Department of Computer Applications, JSS Academy of Technical Education
NOIDA, Uttar Pradesh, 201301, India

² AIM & ACT, Banasthali University
P.O, Banasthali Vidyapith, Rajasthan, 304022, India

Abstract

Information security is not just to provide an authenticity and integrity to the data, but there is also a need to seek identity, rights of use and origin of information, which may require some degree of process re-engineering. Rarely security technologies like digital signatures can be simply "plugged in" without streamlining the process. In this paper we address the problem of information security and protecting the rights of originator of the structured document from ill-intentioned recipient who can modify the received decrypted information. At sender end, a public key signature is generated using SHA-1 or SHA-2. Signature is embedded into raster image of the document using non-invertible robust public key watermarking technique based on orthogonal signals concepts. The document is then encrypted with public key of the receiver using RSA algorithm to achieve confidentiality and authorization. The proposed scheme uses correlation analysis to detect embedded signature to authenticate message. This scheme also uses Gauss-Jordan method to derive the signature from the watermarked image to verify ownership. The study is corroborated with result and application of the proposed technique to prevent forgery and alteration in e-cheque document.

Keywords: *Digital Signature, watermarking, Information Security, Rights Protection, cheque alteration, signature forgery.*

1 Introduction

Over the past few years there has been tremendous growth in computer networks especially in the field of World Wide Web. This phenomenon coupled with the exponential increase of computer performance, has facilitated on-line business operations like shopping, trading, cheque truncation, bill presentment. Due to massive use of personal computers, network and the Internet, new features of security are in need. In addition to confidentiality, authentication, integrity and control, one must

think of new security requirements like protecting the rights of originator against tampering and illegal distribution of the information by the intended recipient, as an ill intentioned authorized recipient can modify and redistribute the decrypted information.

It is well known that cryptography deals with unauthorized access but there are functional limitations like requirement of global clock synchronization, handshaking and costly tamper proof hardware. Digital watermarking is a technique based on digital signal processing which inserts extra signal to digital contents for discouraging illicit modification and distribution of information and to authenticate watermarked contents. But, digital watermarking has the following limitations: -

- (a) No transmission security – due to lack of public key algorithms.
- (b) Text information - Due to binary block format of the text, embedding new bits in the text may introduce irregularities that are visually noticeable.

This paper presents a technique, which contains strengths of digital signature and digital watermarking both so as to provide a secure transmission of messages. Thus the rights of sender on digital content are protected. Figure 1 illustrates an approach that uses raster representation of the document in which digital signature is embedded as watermark. Public key signature protects the document from any intruder, while embedding it as resilient, non-invertible and robust watermark prevents non-trusted receiver to modify the contents of the document.

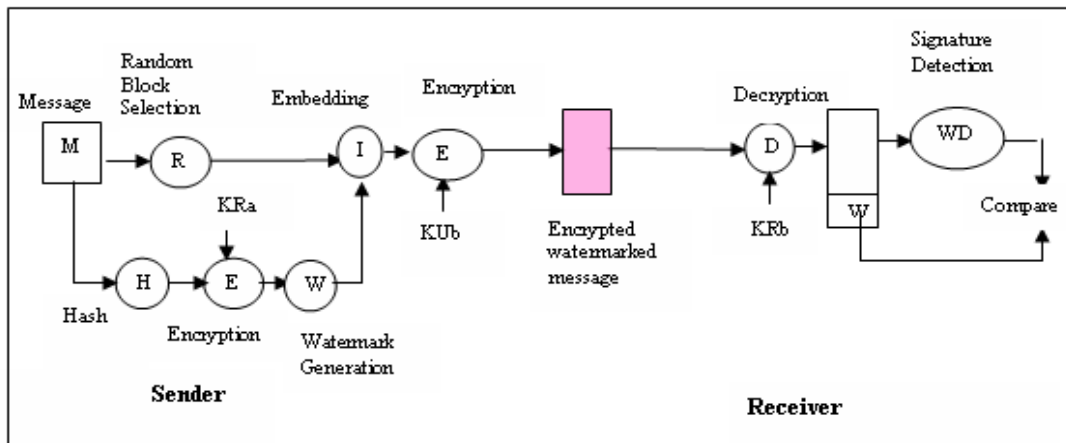


Figure 1 Public Key Cryptosystem with embedded digital signature

The rest of the paper is organized as follows. Section 2 presents digital signatures and watermarking, section 3 describes digital signature generation and embedding procedures, section 4 contains detection of watermark to prove authenticity, and section 5 contains verification of watermark to prove ownership, experimental results are then discussed in section 6 for the purpose of performance evaluation. Conclusion will be given in section 7.

2 Digital Signatures and Watermarking

The ownership protection, authentication and integrity of structured document is necessary and important. Encryption and digital signature techniques protect against eavesdroppers, for sure, but the main attacks are likely to be from validly connected end-users who go on to redistribute the received data more than they are entitled to. Digital signature uses “Public-Key Cryptography” which employs an algorithm using two different but mathematically related “keys” one for creating signature, and, another for verifying signature. Compare this to information hiding the cryptographic signature is embedded into the information itself. Watermarking [1] is a security technique in context of protecting content of information from authorized user. It is as old as paper production and protects rights of author/originator. This technique is basically used to identify any processing and modification in the contents.

2.1 Digital Signatures

Digital signatures have been accepted in several national and international corporations, banks and government agencies. The fundamental process involved in digital signature is a hash function. A number of hash functions are proposed in the literature. The MD5 message digest algorithm,[2] was developed by Ren Rivest at MIT. MD5 generates a 128 bits message digest out of a variable length message. Another hash algorithm SHA (Secure Hash Algorithm) was developed by National Institute of Standards and Technology (NIST) and published as a federal information processing standard [3] in 1993. Revised version of SHA is implemented in C language and referred as SHA-1 [4]. It generates 160 bits message digest. SHA-1 has achieved level of Standard because it generates 32 bits longer message digest than MD5, using a brute force technique for a given digest the difficulty in achieving message is of the order of 2^{160} operations in comparison to 2^{128} operations in MD5. In the draft FIPS 180-2 NIST published SHA-2 as a new version of secure hash algorithm. SHA-2 offers, SHA-1, SHA-256, SHA-384 and SHA-512. In other words SHA-2 may have outputs 160, 256, 384, and 512 bits of message digest. However, SHA-2 algorithm uses fixed and predefined parameters that may be vulnerable to attack.

Digital signature can save the message from third parties [5] but once an encrypted message is at receiver end, an ill-intentioned receiver can

easily decrypt, modify and distribute the message for commercial benefits. This means the sensitive information in these messages cannot be protected from modification and redistribution from the authorized receiver using encryption, access restriction and hiding information behind firewalls.

2.2 Digital Watermarking

A digital watermark is a distinguished piece of information that is adhered to the data that it is intended to protect. Several embedding techniques [1, 6-8] have been specially developed for use with text but most of these techniques either change word or line spacing or make change on the character boundary which require original document to detect watermark to authenticate sender. These techniques cannot be simply used to embed digital signature due to involvement of integrity issues with digital signature applications.

Tao Chen, et al suggests a combined digital signature and digital watermarking scheme [9] for image authentication and content protection. In this scheme content dependent random k bits are extracted from N blocks of image to obtained $K \times N$ bits signature, which is embedded back to the image using secret key. Due to requirement of large number of keys this method cannot be used in applications requiring transmission of data.

Ding Huang presents a text watermarking technique [10] that expands and shrinks widths between words to represent inter word distance, as sine wave. In this method sine wave is coded as watermark. This technique cannot be used to send confidential message, as it does not use any key.

Chang & Chang presented a sender-buyer protocol [11] where digital signature containing sender, buyer and trading information is embedded in the image as barcode image. This scheme protects the embedded trading message and ensures integrity of image but does not authenticate the sender, as digital signature is not based on content of the information.

Cor et al [12] proposed secure spread spectrum watermarking scheme. A two-dimensional spectrum signal is generated. 128 low bits of the

spectrum signal are modulated with 128 bits of the owner's secret key. Adding modulated signal back to the image generates the watermark signal. Inverting spectrum signal, which is then added to the image, generates watermark signal. Drawbacks of this scheme are (1) it requires original image to detect the watermark and (2) Every time new binary key is needed to protect new image.

Natrajan presented a paper for watermarking of digital images to detect or verify ownership [13]. In this method most common RSA & DSS public key signature generation algorithms are used to generate public and private keys of user. This method involves computing message digest using MD5 of image I of M rows and N columns. Message digest is encrypted with private key to generate digital signature. Low order bits of DS are modulated to as watermark and inserted back into the image.

We can summaries that, in order to protect document integrity and rights of owner on the document the crypto signature should be content based and public in order to avoid the large number of secret keys. Secondly such a scheme should not require original document to detect and verify the ownership and should be computationally inexpensive.

The goal of this work is to design a cipher model that contains strengths of digital signature and digital watermarking both to provide secure structured document transmission and to detect and verify ownership to prevent alteration and forgery. The approach uses raster representation of the document in which digital signature is embedded as watermark. Public key digital signature protects the document from third party while embedding it as watermark prevents non-trusted receiver to modify the contents of document.

3. Embedding Digital Signature

3.1 Image representation of a message

The process starts with calculating size of the text information and then converting it into its digital image representation. Input text is stored in string format before conversion. Size of the text is calculated in the form of an invisible drawing in the context of memory device. The

height and width are calculated as shown in figure 2..

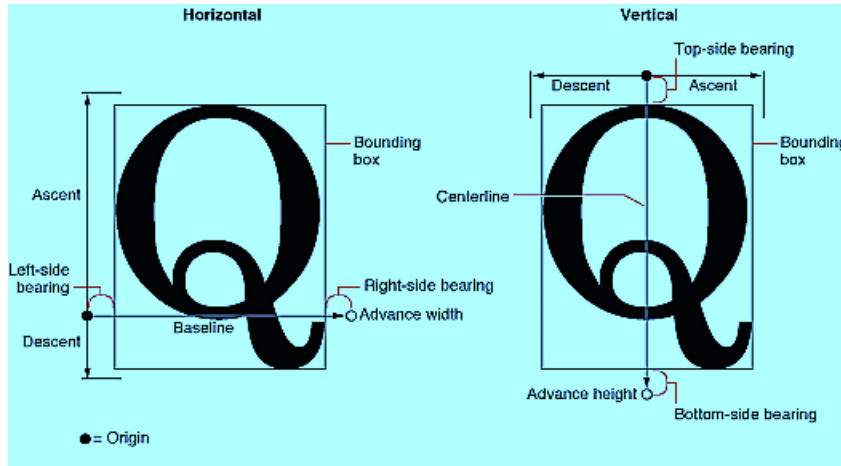


Figure 2: Image size Measurement

$$\text{Image height} = (\text{Ascent} + \text{Descent} + \text{bearing}) * \text{No. of lines in text message} \quad (1)$$

$$\text{Image width} = \text{Max} (x [i]); 0 \leq i \leq \text{no. of lines} \quad (2)$$

True color RGB model is used to represent image as a bit frame of size width*height, where, each square represents a value of bit as function $f(x, y)$.

$$\{f(x, y) = [0,1], | x=0 \text{ to width}, y=0 \text{ to height}\} \quad (3)$$

A total number of 32 frames for a single image are used [14]. The first 8 frames represent transparency; the next 24 frames (8 per color) are used to represent Red, Green and Blue colors respectively. The binary values (0 or 1) in corresponding bits from each of the 32 bit planes result in a binary number to represent pixel's intensity level from 0 to $2^{32}-1$ (full intensity).

For each bit, in all 32 bit frames, value of function $f(x, y)$ is set to 0 to create a white background image.

$$\{f(x, y) = 0 | x=0 \text{ to width}, y=0 \text{ to height}\} \quad (4)$$

Value of function $f(x, y)$ is manipulated at a specific location in all the bit frames to draw text pattern on the background image. Intensity of the image is set in all 32-bit frames to get a specific pixel value [15-17]. Values of pixels stored in

memory are grabbed into a vector of size width * height.

3.2 Generation and Embedding of Digital signatures

This process starts with calculating a message digest from two-dimensional message signal M of m rows and n columns. One-way hash function H operates on input message M of arbitrary length and returns a fixed length hash value h , i.e. $H(M) = h$. It has additional characteristics as follows:

- (i) Given M it is easy to compute h ,
- (ii) Given h it is hard to compute $M' /$ such that $H(M') = h$
- (iii) Given M it is hard to compute another message M' such that $H(M) = H(M')$.

Several methods are developed to find hash function [2-4]. Here SHA-1 algorithm is used to generate unique 160 bits.

Then RSA algorithm is used to encrypt fixed length message digest using owner's private key to generate owner's public key signature vector [5]. Since RSA algorithm is based on the fact that there is insufficient way to factorize very large number, deducing the RSA key, therefore, requires very high computer processing time. RSA algorithm has also become de facto standard for industrial strength and built into many of the software products like Netscape Navigator and Internet Explorer.

Next, the bits of digital signature are modulated and transformed to compute watermark signal. Length of the watermark signal may be same as that of digital signature or it may be based on first, middle or last bits of the digital signature as long as they are consistent. This selection is based on the criteria that too small Watermark signal is vulnerable to attack and too large watermark signal takes large computer power.

Embedding watermark signal X_s into message M involves selecting a random block of m non-overlapping continuous rows and averaging these m rows to find average row vector R referred to as reference vector. Original watermark signal X_s is orthogonalized with respect to vector R to make inserted signal independent from the reference signal and eliminate cross talk [18]. Thus, the vector W_s' constructed out of W entries by modulating digital signature is [12, 19, 20]

$$W_s' = X_s - (X_s \cdot R) R \quad (5)$$

A gain factor is calculated from W_s' across all m rows to ensure that strength of the watermark varies smoothly.

$$i = c \cos(2\pi i / m) W_s' \quad (6)$$

Value of c is adjusted to maintain quality metric PSNR to minimum 30 DB, to avoid white visible marks on message signal. This small scaled version of the W_s' is added back to m rows of the original signal to generate watermarked signal M' , where value of the bit function $f'(x, y)$ is given as.

$$\bigcup_{r=i}^{i+m} f'(x_r, y) = \bigcup_{r=i}^{i+m} f(x_r, y) + I(x_{r-i}, y) \quad 7(a)$$

$$\bigcup_{r=0}^{i-1} f'(x_r, y) = \bigcup_{r=0}^{i-1} f(x_r, y) \quad 7(b)$$

$$\bigcup_{r=i+m+1}^{h-1} f'(x_r, y) = \bigcup_{r=i+m+1}^{h-1} f(x_r, y) \quad 7(c)$$

where $0 \leq \text{random}(i) \leq w - m$

Other blocks of m rows can be selected pseudo randomly to embed additional watermarks using same X_s signal. All X_s and corresponding reference vectors are stored for detection purpose.

3.3 Encrypting watermark signal

RSA algorithm [5] is used to further encrypt watermarked signal M' using public key (d, n) of the receiver to achieve data integrity and confidentiality over network

$$M = \{f'(x, y) \mid x = 0 \text{ to width, } y = 0 \text{ to height}\}$$

$$C = M^d \text{ mod } n \quad (8)$$

4. Detection of Watermark to prove authenticity

The message received is decrypted using private key (e, n) of the receiver to assure for the sender that only authorized receiver can access message and data in the message has not been modified during transmission. To assure the receiver that message has come from the authentic sender. The watermark inserted in the message is detected.

$$M = C^e \text{ mod } n \quad (9)$$

A detection criterion is established using correlation analysis [19, 20]. Watermark is detected using the reference vector R and the watermark vector X_s sent with message itself. X_s is orthogonalized with respect to R to obtain W_s . Watermarked message is scanned from starting in blocks of m rows. An average vector is calculated from each block and orthogonalized with respect to reference vector R to find expected watermark vector EW_s . EW_s is correlated with the watermark vector W_s to test relative closeness.

$$\cos \theta = \frac{EW_s \cdot W_s}{|EW_s| |W_s|} \quad (10)$$

If correlation coefficient is above a threshold value (between 0.5 & 1) then received document

contains the watermark and assumed to have sent by an authentic sender.

Hundreds of random watermarks are synthesized with the same spectral properties as X_s . Correlation of each of these watermarks is computed with watermarked image. If later and former correlations are far apart it is likely that image contains watermark.

5 Verification to prove ownership

Figure 3 presents the procedure to protect rights of sender by deriving watermark from the watermarked image of the signal. Signature derivation will prove ownership of the sender if message is redistributed. At the same time it will restrict authorized receiver to illegally modify the message because in case of modification extracted signature will not match with the original signature of the sender.

Claimant can prove the ownership by presenting original image and the position where watermark was inserted. Gain factor is constructed by subtracting original image from watermarked image and orthogonal watermark W_s' is also constructed.

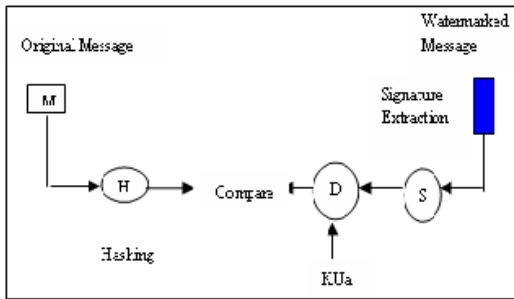


Figure 3: Detection & verification of signature

Vector triple product is applied to find value of X_s from equation (5).

$$(X_s \times R) \times R = (X_s \cdot R) R - (R \cdot R) X_s \tag{11}$$

$$\begin{pmatrix} 1 - \frac{\alpha^2}{\gamma_1^2} & \frac{\alpha \alpha_1}{\gamma_1} & \frac{\alpha \alpha_2}{\gamma_1} & \frac{\alpha \alpha_3}{\gamma_1} \\ \frac{\alpha \alpha_1}{\gamma_1} & 1 - \frac{\alpha^2}{\gamma_2^2} & \frac{\alpha \alpha_2}{\gamma_2} & \frac{\alpha \alpha_3}{\gamma_2} \\ \frac{\alpha \alpha_2}{\gamma_2} & \frac{\alpha \alpha_3}{\gamma_2} & 1 - \frac{\alpha^2}{\gamma_3^2} & \frac{\alpha \alpha_4}{\gamma_3} \\ \dots & \dots & \dots & \dots \\ \frac{\alpha \alpha_3}{\gamma_3} & \frac{\alpha \alpha_4}{\gamma_3} & \frac{\alpha \alpha_5}{\gamma_3} & 1 - \frac{\alpha^2}{\gamma_4^2} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \\ \dots \\ w_n \end{pmatrix} \tag{12}$$

Gauss Jordan method is applied to equation (12) to find components of vector X_s , where m_r is length of vector R . Digital signature S of sender is constructed from X_s after removing all modulations and transformations. If S and X_s are same, ownership of the sender is proved.

6 Implementation and Results

In this section we present the simulation results by implementing orthogonal signals based public-key watermarking algorithm. We used a 32-bit RGB model to represent the cheque image using JAVA advanced imaging classes. We used SHA-1 algorithm to find message digest and RSA algorithm to encrypt message digest. We orthogonalized signature with respect to average vector found from selected block and embedded a scaled version of orthogonalized signature back to the selected block. PSNR was set to minimum 30 DB to avoid white noise. Overall image was encrypted with public key of the recipient to achieve confidentiality and integrity. Signature was detected using correlation analysis. Figure 4 shows 32-bit raster image of the document. Figure 5 shows watermarked image with PSNR 76DB and figure 6 shows the decrypted image. This image is used to detect the watermark using correlation.

The performance of the proposed algorithm is shown in figure 7. Correlation factor is found corresponding to the true signature derived from the original document and corresponding to the 100 randomly selected signatures. The correlation factor corresponding to true signature is between 0.9 and correlation factor corresponding to false signatures is negative or below 0.6.

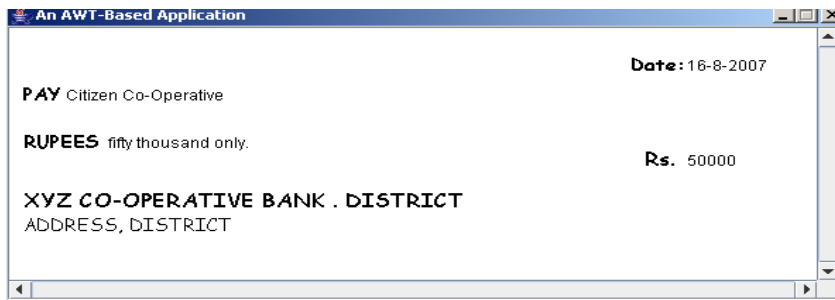


Figure 4: Original Cheque Image

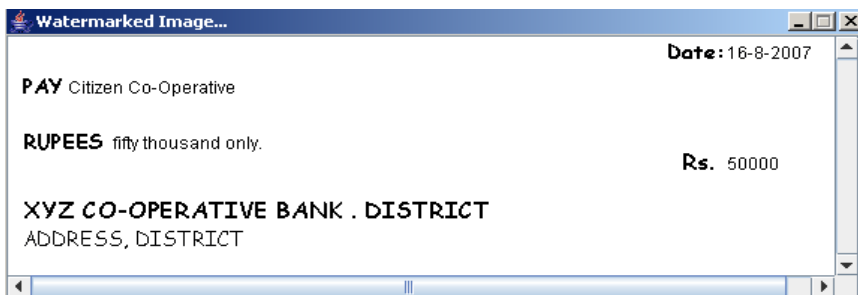


Figure 5: Image of with embedded signature (PSNR -76.98141537143279)

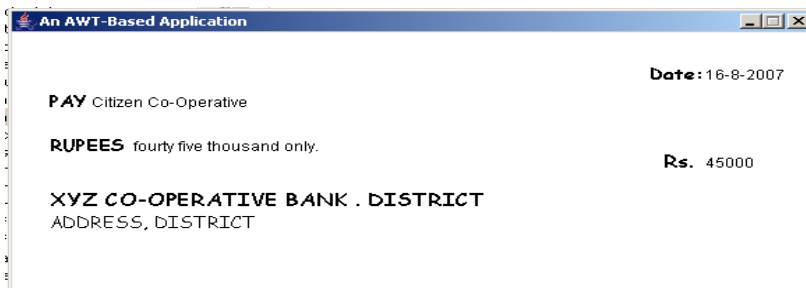


Figure6 6: Received & Decrypted image

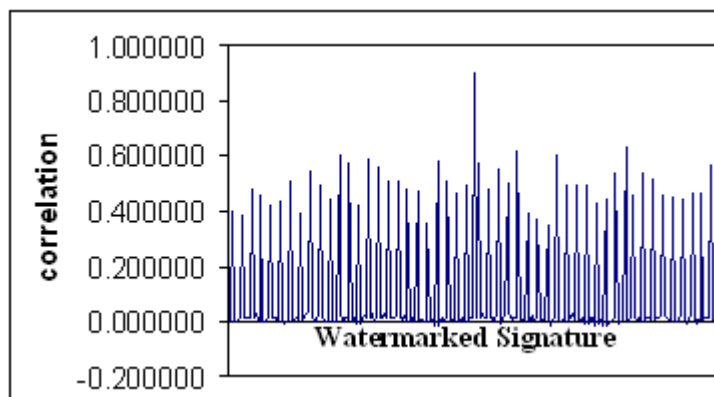


Figure 7: Correlation spread of watermarked image. Central spike corresponds to true signature and other points to randomly generated candidate signature

7 Conclusions

Most of the trading, banking and investment applications are based on exchanging structured documents over global network. For technical excellence and business values of these applications, security of information and sender's rights on information plays an essential role in overall transmission system. Cryptography alone can be an effective solution to all these problems but in most of instances in the form of costly and specialized hardware to create tamper proof devices. In this paper we have presented a software-based approach, which combines digital signature technology with robust watermarking technique to achieve authenticity, confidentiality, integrity and restricting alteration and forgery in information. The proposed technique is tested to prevent forgery of signature and alteration of information in cheques.

References

- [1] Frank Hartung and Martin Kutter , “ Multimedia Watermarking techniques”, Proceeding of the Vol. 87, No. 7, July, 1999.
- [2] Rivest. R , “The MD4 Message Digest Algorithm 1320” MIT and RSA Data Security Inc, April 1992.
- [3] National Institute of Standards and Technology, Fips 180, Federal Information Processing Standards, Secure Hash Standard (SHS), April 1993.
- [4] D.Eastlake .3rd, P.Jones.US , “ Secure Hash Algorithm-1(SHA-1), September,2001.
- [5] W. Stalling , “ Cryptography and network Security Principles and Practice, 4th Edition”, Prentice Hall.
- [6] J.T. Brassil, S. Low and N.F. Maxemchak , “ Electronic Marking and Identification Techniques to Discourage Document copying”, IEEE journal on Selected Areas of Communication,,Vol.13, No. 8,October 1995.
- [7] J.T. Brassil, S.Low and N.F.maxemchak , “ Cpyright Protection for the Electronic Distribution of text Documents”, proceeding of the IEEE
- [8] N.F. maxemchak and S.Low, “ Marking Text Documents”, Proceeding of the IEEE International Conference on Image Processing, Washington. DC, October 26-29, 1997, pp 13-16.
- [9] Tao Chen, Jingchun Wang and Yonglei Zhou, “ Combined Digital Signature and Digital Watermarking scheme for Image Authentication”, in proc IEEE, international Conferences on Info-Tech& Info-Net (ICII2001), Vol 5, pp78-82, 2001.
- [10] Ding Huang, “ Inter word distance changes represented by sine waves for watermarking text images”, IEEE transaction Circuits System Video tech (12), 1237-1245, 2001.
- [11] Ji-Hong Chang and Long-Wen Chang, “ A New Image copyright Protection Algorithm Using Digital Signature of Trading Message and Bar Code Watermark”, Image and Vision Computing 03 New Zealand Proceedings, 26-28, November, 2003.
- [12] Con et al ,”Secure Spread Spectrum Watermarking for Multimedia”, pp 1-33, Copyright, NEC Research Institute, Tech Report95-10.
- [13] Balas Natrajan, “ Robust Public-Key Watermarking of Digital Images”, Computer Systems Laboratory, HPL, 97-118, October 1997.
- [14] D.F.Rogers and J.A.Adams , “ Mathematical Elements for Computer graphics”, TATA-McGraw-Hill, Edition,2002.
- [15] Daniel Sage & Michael Unser , “ Teaching Image Processing programming in JAVA”, IEEE Signal Processing Magazine, November 2003, pp 40-52.
- [16] D. Sage, M User, “ Easy JAVA Programming for Teaching Image Processing”, Proc. Of the 2001 IEEE International Conference on Image Processing (ICIP01) , Thessalonica, Greece, 2001, Vol. 3, pp 298-301.
- [17] D. Roman, M. Fischer and J. Cubillo , “Digital image Processing-An Object-Oriented approach,” IEEE trans. Educ., Vol. 4, pp. 331-333,1998.
- [18] William K. Pratt, ”Digital Image Processing, (Fourth Edition), ” pages 147 - 164. Copyright © 2007 John Wiley & Sons, Inc.
- [19] B.P.Lathi, “Modern Digital and Analog communication system,” Oxford University Press, third edition, 1998, pp 406-416.
- [20] Rafael.C Gonzalez, Richard. E.Woods , “ Digital image processing “Person education, seventh edition(2001), pp111.

Non linear Image segmentation using fuzzy c means clustering method with thresholding for underwater images

Dr.G.Padmavathi, Mr.M.Muthukumar and Mr. Suresh Kumar Thakur.

Abstract

The quality of underwater images is directly affected by water medium, atmosphere, pressure and temperature. This emphasizes the necessity of image segmentation, which divides an image into parts that have strong correlations with objects to reflect the actual information collected from the real world. Image segmentation is the most practical approach among virtually all automated image recognition systems. Clustering of numerical data forms the basis of many classification and system modelling algorithms. The purpose of clustering is to identify natural groupings of data from a large data set to produce a concise representation of a system's behaviour. In this paper we propose fuzzy c means clustering method with thresholding for underwater image segmentation. This paper focuses on comparison of fuzzy c means clustering algorithms with proposed method for underwater images. To evaluate the nonlinear image region segmentation, quantitative statistical measures have been used, such as the gray level energy, discrete entropy, relative entropy, mutual information and information redundancy. The assessment measures will further quantify the impact from image segmentation. The objective assessment approach has the potential to solve other image processing issues. The proposed method gives desirable results on the basis of energy, entropy, mutual information, redundancy, percentage of simplification and computer efficiency for underwater images.

Keywords *underwater images, fuzzy c means clustering, energy, entropy and mutual information*

I INTRODUCTION

Image segmentation is a major step for automated object recognition systems. In many cases, image processing is affected by illumination conditions, random noise and environmental disturbances due to atmospheric pressure or temperature fluctuation. Region segmentation is a crucial step towards automatic segmentation of images. Under some severe conditions of improper illumination and unexpected disturbances, the blurring images make it more difficult for target recognition, which results in the necessity of segmentation. The underwater images have quality degradation due to water dispersion and atmospheric fluctuations. Segmentation is thus needed to clarify feature ambiguity against stochastic disturbances. Region segmentation splits images into regions based on similarity measures, such as pixel intensities, locations and textures or combinations. It categorizes an image into separate parts, which correlates with objects involved.

The theory of fuzzy sets have immediately found its potential application in the fields of pattern recognition and image processing. The fuzzy c-means algorithm generalizes a hard clustering algorithm called the c-means algorithm, which was introduced in the ISODATA clustering method [6]. The (hard) c-means algorithm aims to identify compact, well-separated cluster.

The paper is organized as follows: Section II discusses the need for image segmentation. Section III presents the proposed fuzzy c means clustering algorithm for segmenting underwater images using thresholding. The simulation results with different non-linear parameter evaluation are presented in section IV. Finally, conclusions are given in section V.

II NEED FOR UNDERWATER IMAGE SEGMENTATION

Image segmentation is a major step for automated object recognition systems. In many cases, image processing is affected by illumination conditions, random noise and environmental disturbances due to atmospheric pressure or temperature fluctuations. The quality of underwater images is directly affected by water medium, atmosphere medium, pressure and temperature. This emphasizes the necessity of image segmentation, which divides an image into parts that have strong correlations with objects to reflect the actual information collected from the real world.

Due to unstableness in underwater surroundings, object recognition in underwater is no means an easy task. Light changing or current flow of underwater surroundings often occur rapidly, so the features (shape or color etc) of object may vary in short time and the segmentation process may not give proper results [2]. Therefore subsequent object recognition results are not reliable. The next session explains the algorithm taken for implementation.

III PROPOSED FUZZY C MEANS CLUSTERING METHOD WITH THRESHOLDING

The fuzzy c means clustering method with thresholding is the combination of fuzzy algorithm, c means clustering and thresholding algorithm.

Fuzzy clustering

The goal of a clustering analysis is to divide a given set of data or objects into a cluster, which represents subsets or a group [6]. The partition should have two properties:

- Homogeneity inside clusters: the data, which belongs to one cluster, should be as similar as possible.
- Heterogeneity between the clusters: the data, which belongs to different clusters, should be as different as possible.

The membership functions do not reflect the actual data distribution in the input and the output spaces. They may not be suitable for fuzzy pattern recognition. To build membership functions from the data available, a clustering technique may be used to partition the data, and then produce membership functions from the resulting clustering.

“Clustering” is a process to obtain a partition P of a set E of N objects X_i ($i=1, 2, \dots, N$), using the resemblance or disemblance measure, such as a distance measure d . A partition P is a set of disjoint subsets of E and the element P_s of P is called *cluster* and the centers of the clusters are called *centroids* or prototypes. Many techniques have been developed for clustering data. In this paper c-means clustering is used. It's a simple unsupervised learning method which can be used for data grouping or classification when the number of the clusters is known. It consists of the following steps:

Step 1:

Choose the number of clusters - K

Step 2:

Set initial centers of clusters c_1, c_2, \dots, c_k ;

Step 3:

Classify each vector $X_i = [X_{i1}, X_{i2}, \dots, X_{in}]^T$ into the closest center C_i by

Euclidean distance measure:

$$\|X_i - C_i\| = \min \|X_i - C_i\|$$

Step 4:

Recompute the estimates for the cluster centers C_i Let

$$C_i = [C_{i1}, C_{i2}, \dots, C_{in}]^T,$$

C_{im} be computed by:

$$C_{im} = \frac{\sum X_{li} \in \text{cluster}(i^{x\text{lim}})}{N_i}$$

where N_i is the number of vectors in the i -th cluster.

Step 5:

If none of the cluster centers ($C_i = 1, 2, \dots, k$) changes in step 4 stop; otherwise go to step 3.

C-means algorithm

The criterion function used for the clustering process is:

$$J(v) = \sum_{k=1}^n \sum_{x \in C_i} |x_k - v_i|^2,$$

where v_i is the sample mean or the center of samples of cluster i , and $v = \{v_1, v_2, \dots, v_c\}$.

In the hard clustering process, each data sample is assigned to only one cluster and all clusters are regarded as disjoint collection of the data set. In practice there are many cases, in which the clusters are not completely disjoint and the data could be classified as belonging to one cluster almost as well to another. Therefore, the separation of the clusters becomes a fuzzy notion, and representation of the data can be more accurately handled by fuzzy clustering methods. It is necessary to describe the data in terms of fuzzy clusters. The criterion function used for fuzzy C-means clustering is

$$J(v) = \sum_{i=1}^c \sum_{k=1}^n u_{ik}^m |x_k - v_i|^2,$$

where:

X_1, \dots, X_n - 'n' data sample vectors;

V_1, \dots, V_c - 'c' denotes cluster centers (centroids);

$U = U_{ik}$ $c \times n$ matrix, where u_{ik} is the i -th membership value of the k -th input sample x_k , and the membership values satisfy the following conditions:

$$0 \leq u_{ik} \leq 1; \quad i = 1, \dots, c; \quad k = 1, \dots, n;$$

$$\sum_{i=1}^c u_{ik} = 1; \quad k = 1, \dots, n;$$

$$0 < \sum_{k=1}^n u_{ik} < 1; \quad i = 1, \dots, c;$$

$m \in [1, \infty)$ is an exponent weight factor.

The Fuzzy Logic Toolbox command line function, fcm, starts with an initial guess for the cluster centers, which are intended to mark the mean location of each cluster. The initial guess for these cluster centers is most likely incorrect. Next, fcm assigns every data point a membership grade for each cluster. By iteratively updating

the cluster centers and the membership grades for each data point, fcm iteratively moves the cluster centers to the right location within a data set.

Thresholding

This iteration is based on minimizing an objective function that represents the distance from any given data point to a cluster center weighted by that data point's membership grade. Here fuzzy c means clustering [3] is used based on thresholding. It works better than ostu method [4]. In normal fuzzy c means clustering the segmented part cannot be seen clearly. For that reasons, thresholding is applied to extract the segmented image part. Hence, the annexure I gives the clarity of underwater images after applying the thresholding method, this have proposed in this paper. Aneexure I gives the original underwater images and image after applying fuzzy c means clustering and fuzz c means clustering method with threshold.



Fig 1 original underwater Titanic image

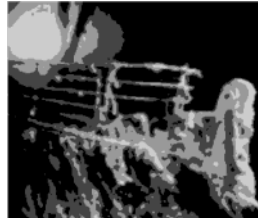


Fig 2 After applying FCM



Fig 3 After Applying FCMT

From the figure it can be observe that the difference between the normal fuzzy c means clustering and fuzzy c means threshold for underwater images. The fuzzy c means threshold method gives better image when compare to normal fuzzy c means clustering.

IV. EXPERIMENTAL SETUP AND EVALUATION

To test the accuracy of the segmentation algorithms, three steps are followed.

- i) First, an underwater image is taken as input.
- ii) Second, segmentation algorithm is applied for underwater image.
- iii) Third, the non linear objective assessment is applied for fuzzy c means algorithm, for evaluation of underwater images.

The reconstruction of an image has the dimensions of 256 pixel intensity. The images in this contain a wide variety of subject matters and textures. Most of the images used are ship wreck, moor chain and mine in sonar images. The non linear assessment applied must be less value for an better image segmentation.

To estimate the quality of the reconstructed images, following non linear objective assessment parameters are used.

The different non linear objective assessment parameters used for evaluation are ,

- i.) Energy
- ii.) Relative Entropy (RT)
- iii.) Discrete Entropy (DE)
- iv.) Mutual Information (MI)
- v.) Normalized Mutual Information (NMI)
- vi.) Redundancy(RD)

i.) Energy

The gray level energy indicates how the gray levels are distributed. It is formulated as,

$$E(x) = \sum_{i=1}^x p(x)$$

where E(x) represents the gray level energy with 256 bins and p(i) refers to the probability distribution functions, which contains the histogram counts. The energy reaches its maximum value of 1 when an image has a constant gray level [2].

ii.) Relative Entropy

Suppose that two discrete probability distributions of the images have the probability functions of p and q, the relative entropy of p with respect to q is then defined as the summation of all possible states of the system, which is formulated as,

$$d = \sum_{i=1}^k p(i) \log_2 \frac{p(i)}{q(i)}$$

iii.) Discrete Entropy (DE)

The discrete entropy is the measure of image information content, which is interpreted as the average uncertainty of information source. It is calculated as the summation of the products of the probability of outcome multiplied by the log of the inverse of the outcome probability, taking into considerations of all possible

outcomes $\{1, 2, \dots, n\}$ in the event $\{x_1, x_2, \dots, x_n\}$, where n is the gray level; $p(i)$ is the probability distribution, considering all histogram counts. It is formulated as

$$H(x) = \sum_{i=1}^k p(i) \log_2 \frac{1}{p(i)} = -\sum_{i=1}^k p(i) \log_2 p(i)$$

For image processing, the discrete entropy is a measure how many bits needed for coding the image data, which is a statistical measure of randomness. The maximal entropy occurs when all potential outcomes are equal. When the outcome is certainty, the minimal entropy occurs which is equal to zero. The discrete entropy represents average amount of information conveyed from each individual image.

iv.) Mutual Information (MI)

The notion of the mutual information can be applied as another objective metric. The mutual information acts as a symmetric function, which is formulated as,

$$\begin{aligned} I(X, Y) &= \sum_{XY} P_{XY}(X, Y) \log_2 \frac{P_{xy}(X, Y)}{P_x(X)P_y(Y)} \\ &= -\sum_x P_x(X) \log_2 P(X) + \sum_{x,y} P_{xy}(X, Y) \log_2 \frac{P_{xy}(X, Y)}{P_x(X)P_y(Y)} \\ &= H(X,) - H(X | Y) \end{aligned}$$

where $I(X; Y)$ represents the mutual information; $H(X)$ and $H(X|Y)$ are entropy and conditional entropy values. It is interpreted as the information that Y can tell about X is equal to the reduction in uncertainty of X due to the existence of Y . At the same time, it also shows the relationship of the joint and product distributions. The results are shown in Table

v.) Normalized Mutual Information (NMI)

The normalized mutual information is a well defined measure covering contents from both discrete entropies and mutual information. It is formulated as

$$NMI = \frac{I(X; Y)}{\sqrt{H(X), H(Y)}}$$

where $I(X, Y)$ is the mutual information; $H(X)$ and $H(Y)$ are the discrete entropies

Table 1 shows the performance evaluation of original image and segmented image using non linear objective assessments like energy, entropy and mutual information.

vi.) Redundancy (RD)

Another symmetric information measure can be used to indicate redundancy in image segmentation. It reaches the minima of zero when all variables are independent. It is formulated as

$$RD = \frac{I(X; Y)}{H(X) + H(Y)}$$

where $H(X)$ and $H(Y)$ are entropies of two images and $I(X; Y)$ is the mutual information.

Table 1 Performance evaluation using fuzzy c means clustering method

Input Image	Non linear Objective Assessments	Original image	Fuzzy C Means Clustering(FCM)	Fuzzy C means Clustering plus thresholding (FCMT)
Underwater Titanic Image	Energy	0.8952	1.7324	0.1708
	Relative Entropy	0.4562	0.3392	0.0495
	Discrete Entropy	0.099	0.2472	0.1032
	Mutual Information	0.9841	1.7315	0.2062
	Normalized Mutual Information	1.2052	1.292	1.2492
	Redundancy	1.5234	0.9862	0.5000
	Computer efficiency in sec.	5.7560	3.6202	2.9606

Like that more number of underwater images are taken for experimentation and the results are give desirable for fuzzy c means clustering method with thresholding.

From table, in image segmentation, the less value of the non linear objective assessment like energy, relative entropy, discrete entropy, mutual information, normalized mutual information, redundancy and computer efficiency gives the Fuzzy C Means threshold (FCM threshold) method is better for underwater images when compare to Fuzzy C Means (FCM) clustering. When compare to original image fuzzy method gives simplified value. The percentage of simulation is also calculated. Its varied from 52% to 95% and the computer efficiency is also calculated using time in seconds. When compare to all performance evaluation it can be say that fuzzy c means threshold method give most suitable results when compare to fuzz c means method.

V CONCLUSION

The quality of underwater images is directly affected by water medium, atmosphere medium, pressure and temperature. This emphasizes the necessity of image segmentation, which divides an image into parts that have strong correlations with objects to reflect the actual information collected from the real world. Image segmentation are most practical approaches among virtually all automated image recognition systems. Clustering of numerical data forms the basis of many classification and system modelling algorithms. The purpose of clustering is to identify natural groupings of data from a large data set to produce a concise representation of a system's behaviour. In this paper the proposed fuzzy c means threshold clustering method gives desirable results when compare to FCM method by using non linear assessment like energy, relative entropy, discrete entropy, mutual information, normalized mutual information, redundancy and computer efficiency when compare to fuzzy c means method for underwater images...

REFERENCES

- [1]. Wen-Xiong Kang, Qing-Qiang Yang, Run-Peng Liang, "The Comparative Research on Image Segmentation Algorithms," First International Workshop on Education Technology and Computer Science, pp.703-707, , vol. 2, 2009.
- [2].Zhengmao ye, "objective assessment of Nonlinear Segmentation Approaches to Gray Level Underwater Images", ICGST-GVIP Journal, pp. 39-46, No.2, Vol. 9, April 2009.
- [3] Y. Ye, Z. Ye, J. Luo, P. Bhattacharya, H. Majlesein, R. Smith, "On Linear and Nonlinear Processing of Underwater, Ground, Aerial and Satellite Images", IEEE International Conference on Systems, Man and Cybernetics, pp.3364-8, Oct.10-12, 2005.
- [4] R. Gonzalez, R. Woods, "Digital Image Processing," 2nd Edition, Prentice-Hall, 2002.
- [5] Mr. S. K. Korde Mrs. K.C. Jondhale, "Hand Gesture Recognition System Using Standard Fuzzy C-Means Algorithm for Recognizing Hand Gesture with Angle Variations for Unsupervised Users", IEEE, First International Conference on Emerging Trends in Engineering and Technology, pp. 681-685, Nov 11 2008.
- [6] Rumiana Krasteva "Bulgarian Hand-Printed Character Recognition Using Fuzzy C-Means Clustering", Bulgarian Academy of sciences problems of engineering cybernetics and robotics, 53, pp. 112-117, 2002.
- [7] Weina Wang, Yunjie Zhang, Yi Li and Xiaona Zhang, "The Global Fuzzy C-Means Clustering Algorithm", Proceedings of the 6th World Congress on Intelligent Control and Automation, pp.33604-3607, June 21 - 23, 2006,.
- [8] A.H.Hadjamthi, M.M.Hmayanpour and S.M.Ahadi, "Robust weighted fuzzy c means clustering", IEEE International Conference on Fuzzy Systems, pp. 306-311, 2008.




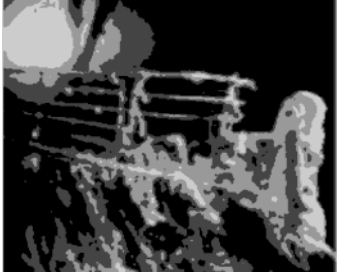





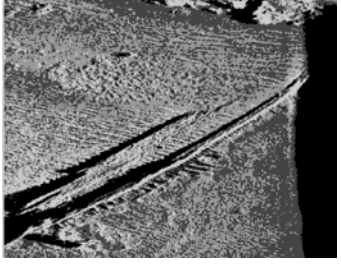

Dr. Padmavathi Ganapathi is the Professor and Head of Department of Computer Science, Avinashilingam University for Women, Coimbatore. She has 21 years of teaching experience and one year Industrial experience. Her areas of interest include Network security and Cryptography and real time communication. She has more than 80 publications at national and International level. She is a life member of many professional organizations like CSI, ISTE, AACE, WSEAS, ISCA, and UWA. She has five funded projects from UGC and DRDO

Mr.M.MuthuKumar. received the diploma in ECE.from Arsan Ganesan Polytechnique College Sivaksi and B.E (EIE) degrees from KCET virudhunagar in 2004 and 2007 respectively.he is currently working as a Research staff in Department of Computer Science in Avinashilingam University for women and has two year of research experience. His research interests are image and signal processing. he has 6 publications at national level and international level..

Mr.SK.Thakur is the Joint Director at Directorate of Naval Research & Development, DRDO HQ, New DelhiDeputy Director at Sectt. of Naval Research Board, New Delhi. He has More than 25 years of experience as a Naval Officer with Indian Navy. Experience in Policy Making & Goal Monitoring, Project Development & Monitoring, Equipment Maintenance & testing, Finance & Budgeting, Liaison with indigenous & foreign firms, Crisis & planned Management, Personnel & Administration; and Instructor/Teacher as Directing Staff; and Research & Development aspects.Experience of working with Research Personnel/Senior professors of IITs/IISc and Scientists from various R&D Institutions.and member of broad casting engineer society, new Delhi, member of IEEE and stragetec electronic group.

ANNEXURE I

Underwater image results for fuzzy c means clustering method with thresholding

Original underwater images	Underwater image after applying FCM	Underwater image after applying FCM threshold
		
		
		

A Theoretical Approach to Link Mining for personalization

K.Srinivas¹, L.Kiran Kumar Reddy² and Dr.A.Govardhan³

¹ Department of Computer Science and Engineering, Geethanjali College of Engineering and Technology
Hyderabad, Andhra Pradesh 500007, India

² Department of Computer Science and Engineering, SLC'S IET
Hyderabad, Andhra Pradesh 500028, India

³ Department of Computer Science and Engineering, Jawaharlal Nehru Technological University,
Jagtial, Andhra Pradesh 505327, India

Abstract

An emerging challenge for data mining is the problem of mining richly structured datasets, where the objects are linked in some way. Many real-world datasets describe a variety of object types linked via multiple types of relations. These links provide additional context that can be helpful for many data mining tasks. Links among the objects may demonstrate certain patterns, which can be helpful for many data mining tasks and are usually hard to capture with traditional statistical models. Recently there has been a surge of interest in this area, fuelled largely by interest in web and hypertext mining in personalization.

Keywords: *Link mining, Clustering, categorizer, Indexer, Personalization.*

1. Introduction

There are different traditional data mining tasks such as association rule mining, market basket analysis and cluster analysis commonly attempt to find patterns in a dataset characterized by a collection of independent instances of a single relation. This is consistent with the classical statistical inference problem of trying to identify a model given a random sample from a common underlying distribution. Data which is storing in data warehouse contains heterogeneous data. A key challenge for data mining is tackling the problem of mining richly structured, heterogeneous datasets. These datasets are typically multi-relational; they may be described by a relational database, a semi-structured representations such as XML, or using relational or first-order logic. However, the key commonalities are that the domain consists of a variety of object types and objects can be linked in some manner. In this case, the instances in our dataset are linked in some way, either by an explicit link, such as a URL, or by a

constructed link, such as a join operation between tables stored in a database.

2. Link Mining

Link mining is a newly emerging research area that is at the intersection of the work in link analysis [4; 5], hypertext and web mining [3]. Links have more generically relationships, among data instances are ubiquitous. These links often exhibit patterns that can indicate properties of the data instances such as the importance, rank, or category of the object. In some cases, not all links will be observed. Therefore, we may be interested in predicting the existence of links between instances. In other domains, where the links are evolving over time, our goal may be to predict whether a link will exist in the future, given the previously observed links. By taking links into account, more complex patterns arise as well. This leads to other challenges focused on discovering substructures, such as communities, groups, or common sub graphs. Traditional data mining algorithms such as association rule mining, market basket analysis, and cluster analysis commonly attempt to find patterns in a dataset characterized by a collection of independent instances of a single relation. This is consistent with the classical statistical inference problem of trying to identify a model given a independent, identically distributed (IID) sample. One can think of this process as learning a model for the node attributes of a homogeneous graph while ignoring the links between the nodes. Link mining tasks are broadly categorized into following tasks. They are

1. Object-Related Tasks

- (a) Link-Based Object Ranking
- (b) Link-Based Object Classification

- (c) Object Clustering (Group Detection)
- (d) Object Identification (Entity Resolution)
- 2. Link-Related Tasks
 - (a) Link Prediction
- 3. Graph-Related Tasks
 - (a) Sub graph Discovery
 - (b) Graph Classification
 - (c) Generative Models for Graphs

In personalized web mining, which is considering different types of categorical domains. Personalization can be achieved through link mining by dynamically constructing user-profiles [1].

3. Proposed Algorithm to Construct Dynamic user Profiles using Link Mining

In this algorithm, thesis is concentrating on the hyperlinks of the web and different attributes of the link such as time spent on each link, link type, link category etc.

Process

- Step 1: Get the log file (From server)
- Step 2: Extract the Links and time spent browsing the links
- Step 3: Check for the relevance of the document (t is time of viewing the document, th threshold time, If $t > th$ the document is relevant)
- Step 4: Categorize the documents that are found relevant
- Step 5: Increase the score for the categories in Profile

In the above algorithm active time and passive time should be considered. If any user is visiting a link then finding about how much time he/she is actively reviewing that link (active time) or just visited that link and if he/she disconnects or away out of the desk should be considered (passive) to calculate the threshold time.

4. Architecture for constructing user Profiles

A closely related line of work is hypertext and web page classification. This work has its roots in the information retrieval (IR) community. A hypertext collection has a rich structure that should be exploited to improve classification accuracy. In addition to words, hypertext has both incoming and outgoing links. Traditional IR document models do not make full use of the link structure of hypertext. In the web page classification problem, the web is viewed as a large directed graph. Our objective is to label the category of a web page, based on features of the current page and features of linked neighbours. With the

use of linkage information, such as anchor text and neighbouring text around each incoming link, better categorization results can be achieved.

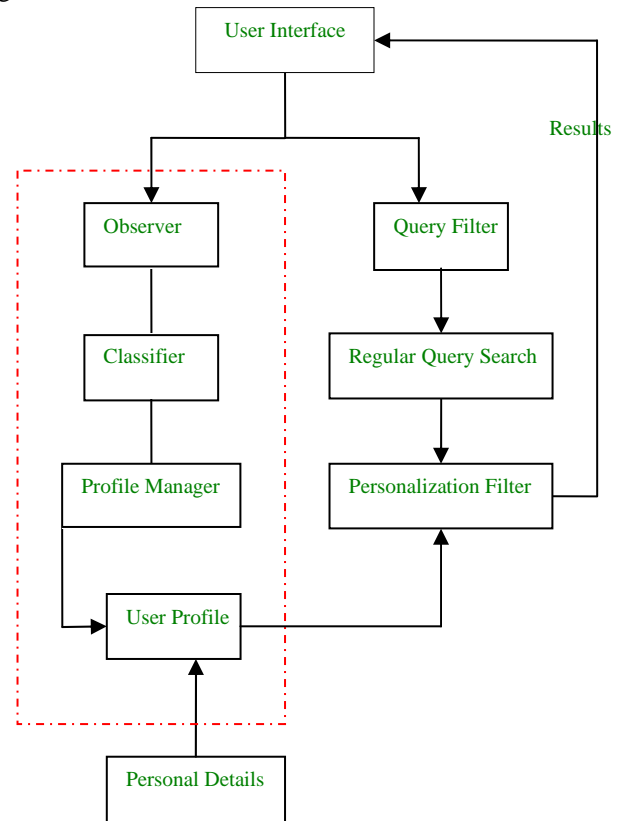


Fig. 1 Architecture for creating dynamic user profiles.

In the given architecture (figure 1) there are different modules with the following functionality.

Observer deals with the details of obtaining the information we need to build the user profile. Like,

- Input Query
- Links the user is visiting
- Time the user is spending on each link
- Length of the content of the link
- Type of the link (PDF, doc, txt, images, audio, video)

Classifier deals with the methodology for query classification, where our aim is to classify queries onto a commercial taxonomy of Web queries with approximately 6000 nodes. Given such classifications, one can directly use them to provide better search results as well as more focused ads. The problem of query classification is extremely difficult owing to the brevity of queries. Observe, however, that in many cases a human looking at the search query and the search results does remarkably well in making sense of it. For instance, in the example

above, sending the query "SD450" to a Web search engine brings pages about Canon cameras, while "nc4200" brings pages about Compaq laptops, hence to a human the intent is quite clear. Of course, the sheer volume of search queries does not lend itself to human supervision, and therefore we need alternate sources of knowledge about the world. Search engines index colossal amounts of information, and as such can be viewed as large repositories of knowledge. Following the heuristic described above, we propose to use the search results themselves to gain additional insights for query interpretation. To this end, we employ the pseudo relevance feedback paradigm, and assume the top search results to be relevant to the query. Certainly, not all results are equally relevant, and thus we use elaborate voting schemes in order to obtain reliable knowledge about the query. For the purpose of this study we first dispatch the given query to a general Web search engine, and collect a number of the highest-scoring URLs. We crawl the Web pages pointed to by these URLs, and classify these pages. Finally, we use these result-page classifications to classify the original query. Our empirical evaluation confirms that using Web search results in this manner yields substantial improvements in the accuracy of query classification. Note that in a practical implementation of our methodology within a commercial search engine, all indexed pages can be pre-classified using the normal text-processing and indexing pipeline. Thus, at run-time we only need to run the voting procedure, without doing any crawling or classification. This additional overhead is minimal, and therefore the use of search results to improve query classification is entirely feasible at run-time.

Another important aspect of our work lies in the choice of queries. The volume of queries in today's search engines follows the familiar power law, where a few queries appear very often while most queries appear only a few times. While individual queries in this long tail are rare, together they account for a considerable mass of all searches. Furthermore, the aggregate volumes of such queries provide a substantial opportunity for income through on-line advertising. For frequent queries, searching and advertising platforms can be trained to provide good results, including auxiliary data such as maps, shortcuts to related structured information, successful ads, and so on. "Tail" queries, however, simply do not have enough occurrences to allow statistical learning on a per-query basis. Therefore, we need to aggregate such queries in some way, and to reason at the level of aggregated query clusters. A natural choice for such aggregation is to classify the queries into a topical taxonomy. Knowing which taxonomy nodes are most relevant to the given query will aid us to provide the same type of support for rare queries as for frequent queries. Consequently, in this work we focus on the classification

of rare queries, whose correct classification is likely to be particularly beneficial.

Profile Manager takes Classifier's inputs and uses them to refine/adapt/update the user profile.

User Profile contains the details and interests of the user.

5. Conclusions

Query classification is an important information retrieval task. Accurate classification of search queries can potentially be useful in a number of higher-level tasks such as Web search and ad matching. Since search queries are usually short, by themselves they usually carry insufficient information for adequate classification accuracy. To address this problem, we proposed a methodology for using search results as a source of external knowledge. To this end, we send the query to a search engine, and assume that a plurality of the highest-ranking search results is relevant to the query. Classifying these results and then allows us to classify the original query with substantially higher accuracy. There has been a growing interest in learning from linked data between objects. Tasks include hypertext classification, segmentation, information extraction, searching and information retrieval, discovery of authorities and link discovery. Domains include the world-wide web, bibliographic citations, criminology and bio-informatics, to name just a few. Learning tasks range from predictive tasks, such as classification, to descriptive tasks, such as the discovery of frequently occurring sub-patterns. There are other different data mining challenges in link mining such as identify of the, Link discovery, common relational patterns, where these topics lie in research area.

References

- [1] Personalized Web Search by Mapping User Queries to Categories- Fang Liu Clement Yu Weiyi Meng Department of Computer Science, Department of Computer Science, Department of Computer Science, University of Illinois at Chicago University of Illinois at Chicago SUNY at Binghamton Chicago.
- [2] D. Jensen. Statistical challenges to inductive inference in linked data. In Seventh International Workshop on Artificial Intelligence and Statistics, 1999 S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569-571, Nov. 1999.
- [3] S. Chakrabarti. Mining the Web. Morgan Kaufman, 2002.
- [4] Personalized Web Search by Mapping User Queries to Categories- Fang Liu Clement Yu Weiyi Meng Department of Computer Science, Department of Computer Science, Department of Computer Science, University of Illinois at Chicago University of Illinois at Chicago SUNY at Binghamton Chicago.

- [5] D. Jensen. Statistical challenges to inductive inference in linked data. In Seventh International Workshop on Artificial Intelligence and Statistics, 1999S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature poly-Si TFT," IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.
- [6] Beitzel, S., Jensen, E., Chowdhury, A., Grossman, D., and Frieder, O. 2004. Hourly analysis of a very large topically categorized web query log. In Proceedings of the 27th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. ACM Press, Sheffield, United Kingdom, 321-328.
- [7] Broder, A., P., Fontoura, M., Gabrilovich, E., Josifovski, V., and Reidel, L. 2008. Search advertising using Web relevance feedback. In CIKM'08.
- [8] Gabrilovich, E. and Markovitch, S. 2007. Harnessing the expertise of 70,000 human editors: Knowledge-based feature generation for text categorization. Journal of Machine Learning Research 8, 2297-2345.

K.Srinivas is a Ph.D. student and received Mater of Technology in Computer Science and Engineering from Jawaharlal Nehru Technological University in 2005 and Bachelor of Engineering in computer science and Engineering from Swami Ramananda Teerth Marathwada University in 2000. He is working as Associate Professor in Geethanjali College of Engineering and Technology and worked as Assistant Professor in Arkay College of Engineering and Technology affiliated to Jawaharlal Nehru Technological University. His main research interests include Data Mining and Information Retrieval.

L.Kiran Kumar Reddy received M.Tech. in Computer Science and Engineering in 2006 and B.E. in Computer Science and Engineering from Swami Ramananda Teerth Marathwada University in 2000. He is working as Associate Professor in Satyam Learning Campus's Institute of Engineering and Technology and worked as Assistant Professor in Arkay College of Engineering and Technology. He is doing research in Data Mining and Information Retrieval.

Dr.A.Govardhan received Ph.D. degree in Computer Science and Engineering from Jawaharlal Nehru Technological University in 2003 M.Tech. from Jawaharlal Nehru University in 1994 and B.E. in from Osmania University in 1992. He is Working as a Principal of Jawaharlal Nehru Technological University, Jagtial. He has Published around 50 papers in various national and international Journals/conferences. His research of interest includes Data Mining, Information Retrieval, Search Engines.

Image Compression Algorithms for Fingerprint System

Preeti Pathak

CSE Department, Faculty of Engineering, JBKP, Faridabad, Haryana, 121001, India

Abstract

Fingerprint-which have been used for about 100 years are the oldest biometric signs of identity. Humans have used fingerprints for personal identification for centuries and the validity of fingerprint identification has been well established. In fact, fingerprint technology is so common in Human Identification that it has almost become the synonym of biometrics. Fingerprints are believed to be unique across individuals and across fingers of same individual. Even identical twins having similar DNA, are believed to have different fingerprints. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies. A major approach for fingerprint recognition today is to extract minutiae from fingerprint images and to perform fingerprint matching based on the number of corresponding minutiae pairings. One of the most difficult problems in fingerprint recognition has been that the recognition performance is significantly influenced by fingertip surface condition, which may vary depending on environmental or personal causes. Addressing this problem this paper propose some extra features that can be used to strengthen the present approaches followed in developing Fingerprint recognition system. To increase security and accuracy we can use Infrared technique and technique to assign a score value to each of extracted minutiae.

Key Terms– Biometric, Minutiae, Binarization, Thinning, Median Filter.

1. Introduction

Biometric authentication has been receiving extensive attention over the past decade with increasing demands in automated personal identification. Biometric is to identify individuals using physiological or behavioral characteristics, such as fingerprint, face, iris, retina, palm-print, etc. Among all the biometric techniques, fingerprint recognition [1] is the most popular method and is successfully used in many applications. Typical fingerprint recognition methods employ feature-based image matching, where minutiae (i.e., ridge ending and ridge bifurcation) are extracted from the registered fingerprint image and the input fingerprint image, and the number of corresponding minutiae pairings between the two images is used to recognize a valid fingerprint image [1]. The feature-based matching provides an effective way of identification for majority of people. The

minutiae based automatic identification technique first locates the minutiae point and matches their relative placement in a given finger and the stored template, shown in figure 1.

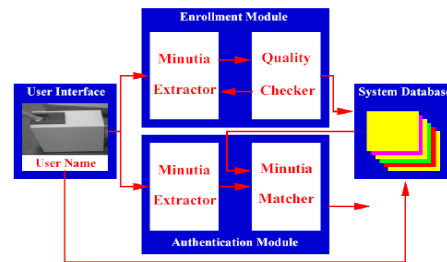


Fig. 1: Fingerprint Recognition System

The fingerprint image may be obtained from a thumb pad fingerprint scanner device scanning at 500 dpi [2]. A good quality fingerprint contains between 60 and 80 minutiae, but different fingerprint have different number of minutiae. A fingerprint image essentially consists of a set of minutiae on the plane. Minutiae are the terminations and bifurcations of ridge lines in a fingerprint image. In order to extract these minutiae, we have to undergo the operation linearization followed by the process of thinning. Thus, the set minutiae those are well defined and more prominent than the rest are given higher relevance and importance in the process of minutiae matching.



Fig.2 : Terminations and bifurcations of ridge lines in a fingerprint image

2. System Architecture

The fingerprint recognition system is shown in figure 3. It consists of four components

1. User Interface (with Infrared Sensor)
2. System Database
3. Enrollment Module
4. Authentication Module

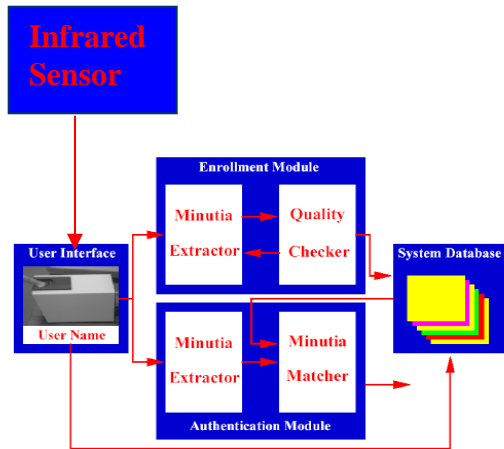


Fig 3 : System Architecture

The user interface provides mechanisms for a user to indicate his/her identity and input his/her fingerprints into the system. Here along with fingerprint scanner the Infrared Sensor will be used. The system database consists of a collection of records, each of which corresponds to an authorized person that has access to the system. Each record contains the following fields which are used for authentication purpose:

- ➔ User name of the person ,
- ➔ Minutiae templates of the person's fingerprint, and other information (e.g., specific user privileges). Alongwith thermal parameter.

The task of enrollment module is to enroll persons and their fingerprints into the system database. When the fingerprint images and user name of a person to be enrolled are fed to the enrollment module, a minutiae extraction algorithm is first applied to the fingerprint images and the minutiae patterns are extracted. A quality checking algorithm is used to ensure that the records in the system database only consist of fingerprints of good quality, in which a significant number (default value is 25) of genuine minutiae may be detected. If a fingerprint image is of poor quality, it is enhanced to improve the clarity of ridge/vally structures and mask out all

the regions that can not be reliable recovered. The enhanced fingerprint image is fed to the minutiae extractor again. The task of authentication module is to authenticate the identity of the person who intends to access the system. The person to be authenticated indicates his / her identity and places his / her finger on the fingerprint scanner ; a digital image of his her fingerprint is captured ; minutiae pattern is extracted from the captured fingerprint image and fed to a matching algorithms which matches it against the person's minutiae templates stored in the system database to establish the identity To increase security and accuracy we can use Infrared technique and technique to assign a score value to each of extracted minutiae.

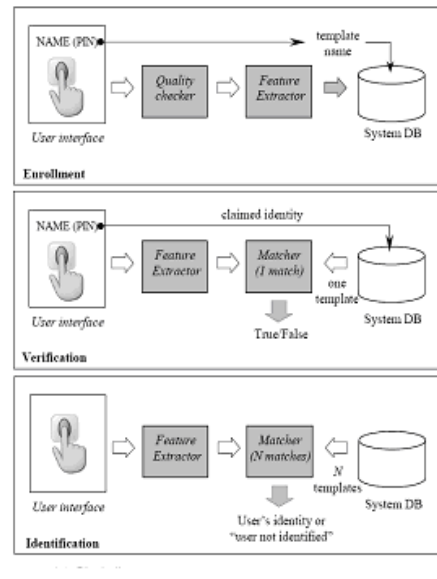


Fig. 4: Block diagrams of Enrollment ,Verification, Identification Task

3. Development of proposed system

Proposed system consist of following sub modules -

3.1 Normalization

By normalizing an image, the colors of the image are spread evenly throughout the gray scale. A normalized image is much easier to compare with other images, and the quality of the image is easier determined.

Normalization is a pixel-wise operation that does not change the clarity of the ridge and valley structures . Normalization reduces the variations in gray level values along ridges and valleys, which facilitates the subsequent processing steps.

Let $I(x; y)$ denote the grayscale value at pixel $(x; y)$, M and

V , the estimated mean and variance of grayscale values in this 64 X 64 window, respectively, and $N(x; y)$, the normalized grayscale value at pixel $(x; y)$. For all the Pixels in the window, the normalized image is defined as:

$$N(x, y) = \begin{cases} M_0 + \sqrt{\frac{V_0 \times (T(x, y) - M^2)}{V}}, & \text{if } |T(x, y) - M| > M \\ M_0 + \sqrt{\frac{V_0 \times (T(x, y) - M^2)}{V}}, & \text{if } |T(x, y) - M| \leq M \end{cases} \quad (1)$$

In Eq. (1), M_0 and V_0 are the desired mean and variance Values, respectively. Normalization is a pixel-wise Operation and does not change the clarity of the ridge and Valley structures. For our experiments, we set the values of both M_0 and V_0 to 100. The values of M_0 and V_0 should be the same across all the training and test sets [7].

3.2 Median Filter

In image processing it is usually necessary to perform high degree of noise reduction in an image before performing higher-level processing steps, such as edge detection. The median filter is a non-linear digital filtering technique, often used to remove noise from images or other signals. The idea is to examine a sample of the input and decide if it is representative of the signal. This is performed using a window consisting of an odd number of samples. The values in the window are sorted into numerical order; the median value, the sample in the center of the window, is selected as the output. The oldest sample is discarded, a new sample acquired, and the calculation repeats.

Median filtering is a common step in image processing. It is particularly useful to reduce speckle noise and salt and pepper noise. Its edge-preserving nature makes it useful in cases where edge blurring is undesirable.

The median filter is also a spatial filter, but it replaces the center value in the window with the median of all the pixel values in the window. The kernel is usually square but can be any shape. An example of median filtering of a single 3x3 window of values is shown below.

Unfiltered values
 6 2 0
 3 97 4
 19 3 10

In order: 0, 2, 3, 3, 4, 6, 10, 15, 97

Median filtered

* * *
 * 4 *
 * * *

Center value (previously 97) is replaced by the median of all nine values. Note that for the first (top) example, the median filter would also return a value of 5, since the ordered values are 1, 2, 3, 4, 5, 6, 7, 8, 9. For the second (bottom) example, though, the mean filter returns the value 16 since the sum of the nine values in the window is 144 and $144 / 9 = 16$. This illustrates one of the celebrated features of the median filter: its ability to remove 'impulse' noise (outlying values, either high or low). The median filter is also widely claimed to be 'edge-preserving' since it theoretically preserves step edges without blurring. However, in the presence of noise it does blur edges in images slightly.

Median filtering is a simple and very effective noise removal filtering process. Its performance is particularly good for removing shot noise. Shot noise consists of strong spike like isolated values.

Shown below are the original image and the same image after it has been corrupted by shot noise at 10%. This means that 10% of its pixels were replaced by full white pixels. Also shown are the median filtering results using 3x3 and 5x5 windows; three (3) iterations of 3x3 median filter applied to the noisy image; and finally for comparison, the result when applying a 5x5 mean filter to the noisy image.

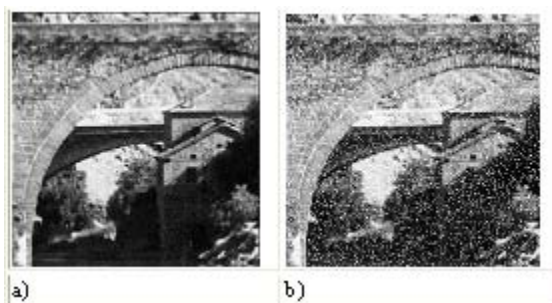


Fig 5: a) Original image; b) Added Shot Noisy at 10%

3.3 Binarization (Regional Average Threshold)

Making an image binary, transforms the gray scale image into a binary image (black and white). Either a global or localized threshold value

is used. Gray level images cannot be operated on for the determination of key features as the range of values of pixel intensities very widely. So it is very difficult to discriminate conspicuously the valleys from the ridges, as well as ridges bifurcations from ridge endings. Hence some half toning technique needs to be applied on the finger print image. A popular technique is that of Threshold of Binarization [3] [4] [5].

In many image-processing applications it is desired to convert the the gray images into white and black (bi-level) image. Thesholding involves looking at each pixel and deciding whether it can be converted into white (0) or black (255), the decision is made by comparing the numerical pixel value against a fixed number called a threshold level (T). If any pixel of image(x ,y) is less than the threshold level (T), the pixel is set to zero (background point), otherwise it is set to 255 (object point).

Algorithm:

1. Divide the image into 4*4 regions.
2. Calculate the average of gray level in the first 4*4 region.
3. Threshold the leftmost region of 4*2 by using average gray level calculated in stage2.
4. Move the 4*4 operation window by 2 pixels to the right . If right edge of the image is reached , then move the window 4 pixels up and return to the left edge .
5. Repeat stage 2 to stage 4 until the entireimage is processed by RAT(Regional average thresholding).

3.4 Thinning

Hear thinning algorithm is based on ridge following. Such an algorithm has a better probability of enhancing the required properties of image . Ridges exist in all finger prints and they form the features either by ending (ridge endings) or by forking bifurcations . In our work we are using black pixels as the ridges in fingerprints. The current work uses thining algorithm which deals with just black pixels, which are between two white pixels [2] [3] [5].

Algorithm:

1. The image is read from bottom left to the right side line by line and the algorithm always tries to find day any of black pixels in the original image . Because it is obvious that any of black pixels may be constituent of ridge.

2. The algorithm finds out (x,y) location of the first block pixel which is not processed yet in the original binary image.
3. A black pixel is inserted into thinned image at (x,y) location (gray pixels) and the black pixel is removed from the original binary image at the location.

Then algorithm looks at the ridge continuity , if there is ridge continuity , it follows the ridge.

3.5 Noise Removal

After applying thinning algorithm we are lift with an image that still has got some noise , i.e. some ridges are not of one pixel width or some other noise , this module is used to remove this noise

In this we check if in the neighborhood of a pixel there are more than five pixels. Less than five pixels imply that this pixel is a ridge end or bifurcation or some part of a ridge. More than five pixels imply that this pixel is associated with some noise.

3.6 Depuration

The image obtained from previous module still not suitable for minutie detection . This module removes some more defects .Depuration of the ridge map involves removal of the spurious elements, identified as undesirable spikes, and to join the broken lines using a smoothening procedure . This depuration process is carried out by simple rules like .

- ➔ To remove small isolated lines.
- ➔ To merge all the lines who have end points with similar direction and the distance between them is small.

Algorithm :

1. First identify the pixel which is a ridge end.
2. Then find out another black pixel in the 7*7 matrix neighborhood of this pixel.
3. If this pixel exists then we find out the slope of two respective ridges at their respective ridge ends in 7*7 matrixes.
4. If the slopes obtained are comparable then join ridge ends by using DDA algorithm.

3.7 Minutiae Extraction

Minutiae extraction was carried out using the crossing number approach. Crossing number of pixel 'p' is

defined as half the sum of the differences between pairs of adjacent pixels defining the 8-neighborhood of 'p'. Mathematically in eq.(2).

$$cn(p) = \frac{1}{2} \sum_{i=1..8} |val(p_{i \bmod 8}) - val(p_{i-1})| \quad (2)$$

Where p0 to p7 are the pixels belonging to an ordered sequence of pixels defining the 8-neighborhood of p and val(p) is the pixel value.

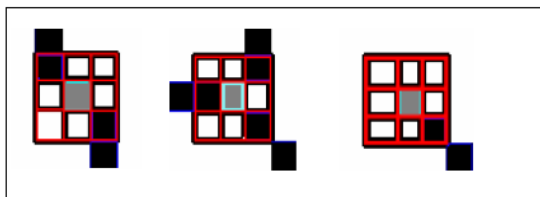


Fig.6: $cn(p)=2, cn(p)=3$ and $cn(p)=1$ representing a nonminutiae region, a bifurcation and a ridge ending

Crossing numbers 1 and 3 correspond to ridge endings and ridge bifurcations respectively. An intermediate ridge point has a crossing number of 2. The minutiae obtained from this algorithm must be filtered to preserve only the true minutiae. The different types of false minutiae introduced during minutiae extraction include spike, bridge, hole, break, Spur, Ladder, and Misclassified Border areas. (See figure 7)

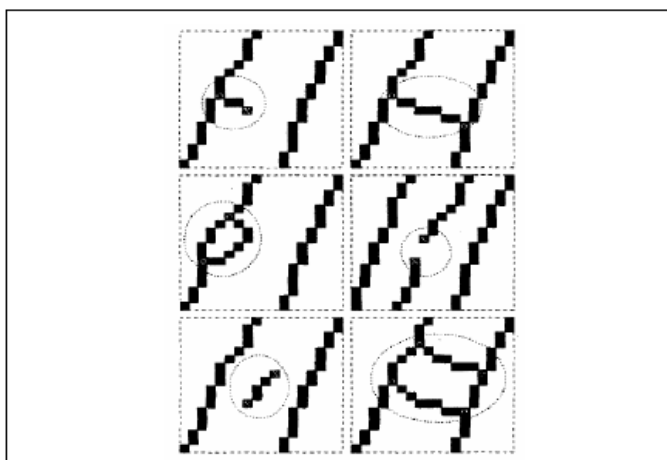


Fig. 7: Types of false minutiae

- A B
 - C D
 - E F
- A. Spike, B. Bridge, C. Hole, D. Break, E. Spur F. Ladder

The number of minutiae in a given area is also limited therefore the minutiae density must also be kept in check. In order to filter out these false minutiae a 3 level-filtering process is applied:

Level 1: Removes the false ridge endings created as a result of the application of minutiae extraction algorithm at the ends of the thinned image.

Level 2: Removes the first five types of minutiae mentioned above using the rule based morphological minutiae filtering approach given by .

Level 3: This stage limits the maximum number of minutiae present in the thinned image to a pre-specified threshold.

A minutiae m is described by the triplet $m=\{x, y, \theta\}$, where x, y indicate the minutiae location coordinates and θ denotes the minutiae orientation, which is the orientation evaluated for the minutiae location from the orientation image obtained during the enhancement process. The minutiae type is not being used during the matching process since minutiae type can be inverted due to enhancement and binarization steps [6].

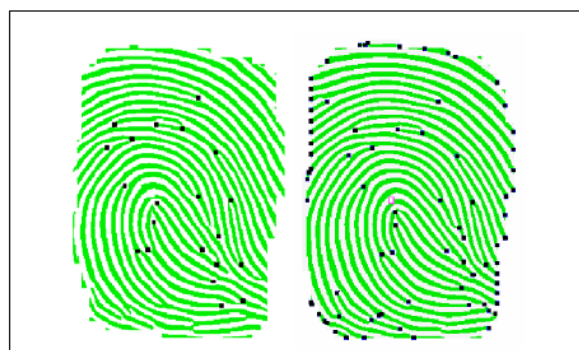


Fig. 8: Filtered and Unfiltered Minutiae Sets

In this process we use text files as databases. We consider three text files for storing the bifurcation information, the ridge information, and the thermal parameters respectively. Every time a new fingerprint image is operated upon, a set of two text files are generated along with another file for keeping information about the person whose fingerprint is under checking. In case of verification, the text files generated are matched with the existing ones and the numbers of matches are displayed.

3.8 Minutiae Matching

Let T and I be the representation of the template and input fingerprint, respectively. Let the minutiae sets of the two fingerprints be given by:

$$\begin{aligned} T &= \{m_1, m_2, \dots, m_n\} \\ I &= \{m'_1, m'_2, \dots, m'_n\} \\ m_i &= \{x_i, y_i, \theta_i\}, i = 1 \dots m \\ m_j &= \{x'_j, y'_j, \theta'_j\}, j = 1 \dots n \end{aligned} \quad (3)$$

A minutia m_j in I and a minutia m_i in T are considered to be matched if their spatial and orientation differences are within specified thresholds r_0 and θ_0 . Minutia matching was carried out by using the approach given in [6]. In this approach the minutiae sets are first registered using a derivative of the Hough transform followed by fingerprint matching using spatial and orientation-based distance computation. The matching algorithm returns a percentage match score, which is then used to take the match-no match decision based on the security criterion [6].

4. Result and discussion

To study the performance of the proposed work, we consider the database containing 350 images. There are 10 different impressions per finger. Here we assume that images should be of good quality with at least 500 dpi and noise level, if any, of the image should be removed by the preprocessing. The performance of the system has shown the efficiency about 97% in 5.8 seconds. It has been seen that when the core point is correctly located, the translation invariant property of features is satisfied and the rotation handled in the matching stage is very fast. As result of which the matching process becomes very fast.

5. Conclusion

The paper presents different steps involved in the development of a fingerprint based person identification and verification system. And the proposed fingerprint recognition system uses both frequency and orientation information available in fingerprint. Due to this, the existing system become

more reliable. This system needs some extra cost and more processing time, but one can not compromise with the security.

References

- [1] D.Maltoni, D.Maio, A.K.Jain, and Prabhakar, "Hand book of fingerprint Recognition". Springer, 2003
- [2] V.Espinosa-Duro., "Minutiae detection algorithm for fingerprint recognition", IEEE Aerospace Electron. Syst. Mag. 17(3), 7-10, 2002
- [3] D. Manolescu, "Feature extraction - a pattern for information retrieval", In Proceedings of the 5th Pattern Languages of Programming, Monticello, Illinois, USA, August 1998.
- [4] A.K.Jain, "Fundamentals of Digital Image Processing", PHI, ISBN-13:978-013336150
- [5] Dario Maio, Davide Maltoni, "Direct Graay-Scale Minutiae Detection In Fingerprints", IEEE Transactions on Pattern Analysis and Machine Intelligence v.ol. 9 n.o.1, pp., 27-40, January 1997
- [6] F.A.Afsar, M.Arif and M.Hussain, "Fingerprint Identification and Verification System using Minutiae Matching", National conference on Emerging Technologies 2004
- [7] Bhupesh Gour, T. K. Bandopadhyaya, Sudhir Sharma, "Fingerprint Feature Extraction Using Midpoint ridge Contour method and Neural Network", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.7, July 2008

About the Author

The Author, Preeti Pathak, working as Lecturer in Department, Faculty of Engineering, JBKP, Faridabad, India. She has received her M.Tech (Comp. Sc. & Tech) from Maharishi Dayanand University, Rohtak along with two other Master degrees, M.Sc. in Physics from Agra University, Agra and M.C.A. (Master in Computer Applications) from IGNOU, New Delhi, INDIA. She has also served as Lecturer in other Eng. Colleges like BSA and Arravali Eng. College Faridabad. She has been involved in many Training, Seminars and conferences. She has also presented her Technical Papers in Two International Conferences and two National Conferences. She has also completed her Training on "Selected Topics in Software Engineering" sponsored by AICTE and HRD of India held in March 18-24, 2010 at IIT, Kharagpur. She has begged many such Certificates and achievements in her educational career. Her research interest includes Software Engineering, Fuzzy System, Image Processing and Computer Networks & Internet Technology.

IJCSI CALL FOR PAPERS NOVEMBER 2010 ISSUE

Volume 7, Issue 6

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas. See authors guide for manuscript preparation and submission guidelines.

Accepted papers will be published online and authors will be provided with printed copies and indexed by Google Scholar, Cornell's University Library, ScientificCommons, CiteSeerX, Bielefeld Academic Search Engine (BASE), SCIRUS and more.

Deadline: 30th September 2010

Notification: 31st October 2010

Revision: 10th November 2010

Online Publication: 30th November 2010

- Evolutionary computation
- Industrial systems
- Evolutionary computation
- Autonomic and autonomous systems
- Bio-technologies
- Knowledge data systems
- Mobile and distance education
- Intelligent techniques, logics, and systems
- Knowledge processing
- Information technologies
- Internet and web technologies
- Digital information processing
- Cognitive science and knowledge agent-based systems
- Mobility and multimedia systems
- Systems performance
- Networking and telecommunications
- Software development and deployment
- Knowledge virtualization
- Systems and networks on the chip
- Context-aware systems
- Networking technologies
- Security in network, systems, and applications
- Knowledge for global defense
- Information Systems [IS]
- IPv6 Today - Technology and deployment
- Modeling
- Optimization
- Complexity
- Natural Language Processing
- Speech Synthesis
- Data Mining

For more topics, please see <http://www.ijcsi.org/call-for-papers.php>

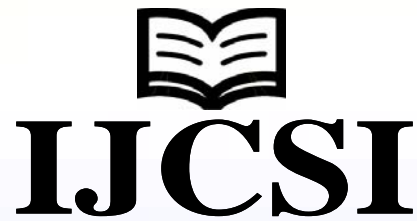
All submitted papers will be judged based on their quality by the technical committee and reviewers. Papers that describe research and experimentation are encouraged.

All paper submissions will be handled electronically and detailed instructions on submission procedure are available on IJCSI website (www.IJCSI.org).

For more information, please visit the journal website (www.IJCSI.org)

© IJCSI PUBLICATION 2010

www.IJCSI.org



The International Journal of Computer Science Issues (IJCSI) is a refereed journal for scientific papers dealing with any area of computer science research. The purpose of establishing the scientific journal is the assistance in development of science, fast operative publication and storage of materials and results of scientific researches and representation of the scientific conception of the society.

It also provides a venue for researchers, students and professionals to submit on-going research and developments in these areas. Authors are encouraged to contribute to the journal by submitting articles that illustrate new research results, projects, surveying works and industrial experiences that describe significant advances in field of computer science.

Indexing of IJCSI:

1. Google Scholar
2. Bielefeld Academic Search Engine (BASE)
3. CiteSeerX
4. SCIRUS
5. Docstoc
6. Scribd
7. Cornell's University Library
8. SciRate
9. ScientificCommons