International Journal of Innovative Technology and Exploring Engineering

ISSN : 2278 - 3075
Website: www.ijitee.org
Volume-6 Issue-7, DECEMBER 2016
Published by:
Blue Eyes Intelligence Engineering and Sciences Publication Pvt. Ltd.

Dr. Durgesh Mishra
Chairman, IEEE Computer Society Chapter Bombay Section, Chairman IEEE MP Subsection, Professor & Dean (R&D), Acropolis Institute of Technology, Indore (M.P.), India

Managing Chair

Mr. Jitendra Kumar Sen
International Journal of Innovative Technology and Exploring Engineering (IJITEE)

Reviewer Chair

Dr. Sanjay Babarao Warkad
Assoc. Professor, Department of Electrical Engineering, Priyadarshini College of Engineering, Nagpur, India

Dr. Ahmed Nabih Zaki Rashed
Assoc. Professor, Department of Electronics and Electrical Communication Engineering, Menoufia University, Menoufia, EGYPT

Dr. Deepali Virmani
Assoc. Professor, Department of Computer Science & Engineering, BPIT, GGSIPU, Rohini, Delhi, India

Dr. M. Subba Rao
Professor, Department of Information Technology, Annamacharya Institute of Technology and Sciences, Kadapa, Andra Pradesh, India

Dr. K.V.L.N. Acharyulu
Professor, Faculty of Science, Dept. of Mathematics, Bapatla Engineering College, Bapatla-522101, Andhra pradesh, India

Dr. Remisetti Rajeswara Rao
Professor & Haed, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Gandipet, Hyderabad, India

Dr. R.R. Mudholkar
Associate Professor, Department of Electronics, Shivaji University, Kodhapu (Maharashtra), India

Dr. Rajesh Kumar U. Sambhe
Assoc. Professor & Head, Mechanical Engineering Workshop Department, Jawaharlal Dard Institute of Engineering and Technology, Yavatmal (Maharashtra), India

Dr. A. Indra
Senior General Manager, Department of Space, Control Centre and Computer Facilities, ISRO Telemetry, Tracking and Command Network, Bangalore (Karnataka), India

Dr. M. Sasikumar
Professor, Department of Electrical & Electronics Engineering, Jeppiaar Engineering College, Chennai (Temil Nadu), India

Dr. Syed Asfandyar Gilani
Research Associate at SCIT Lab, Lahore, Pakistan

Dr. VPS Naidu
Scientist, MSDF Lab, CSIR-NAL, Bangalore-17, India

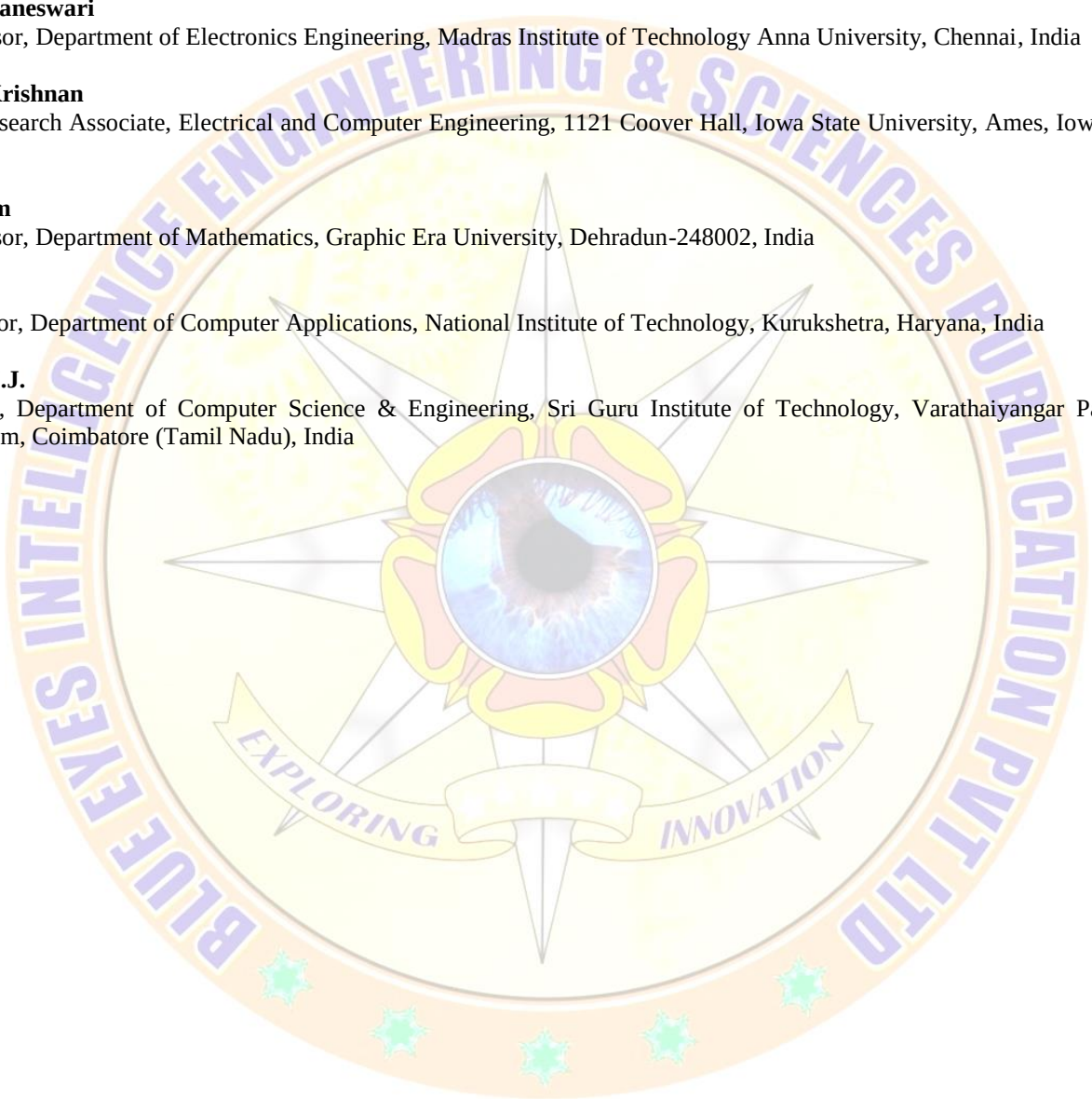
Dr. Kamal K. Mandal
Assoc. Professor, Department of Power Engineering, Jadavpur University, Salt Lake Campus, Kolkata-700098, India

Dr. G. Sreedhar
Associate Professor, Department of Computer Science, Rashtriya Sanskirt Vidyapeetha (Deemed University), Tirupati, (A.P), India

Dr. B. Muthukumar
Assoc.Professor, Department of Information Technology, Kathir College of Engineering, Neelambur, Coimbatore (Tamilnadu), India

Dr. V. Nagarajan
Professor & Head, Department of Electrical and Electronics Engineering, Sona college of Technology, Salem (Tamilnadu), India

Dr. R.Arulmozhiyal
Assoc. Professor, Department of Electronics and Communication Engineering, Adhiparasakthi College of Engineering, Villupuram (Tamilnadu), India



1.

Authors: Amrik Singh, Yoginder Talwar, Ajay Prasad

Paper Title: Highly Secure and Fast AES Algorithm Implementation on FPGA with 256 bit key size

Abstract: The Block cipher AES is a symmetric key cryptographic standard used for transferring block of data in secure manner for server based communication networks, SCADA systems for Oil refinery, Oil and Gas Pipe Lines, and Smart Grids based applications. High level security of data transfer needs long key size i.e. 256 bits, analysis of certain ideas of round key expansion mechanisms from given key data are discussed and the same is implemented in FPGA configuration with 128 bits and 256 bits key size to achieve low latency, high throughput with high security.

Keywords: Advance Encryption Standard, encryption, decryption, FPGA, VHDL, Virtex-5.

References:

1. J. Daemen and V. Rijmen. AES proposal: Rijndael. In AES Round 1 Technical Evaluation, NIST 1998. (see: http:// www.esat.kuleven.ac.be/rijmen /rijndael/, http://www.nist.gov/aes)
2. N ferguson, R. Schroeppel, D. Whiting. A simple algebraic representation of Rijndael Selected Area in Cryptography, SAC 2001, LNCS 2259, Springer-Verlag, 2001, pp.103-111.
3. Courtois, N.T. and J. Pieprzyk: Cryptanalysis of Block Ciphers with over defined Systems of Equations. Accepted by, Asiecrypt 2002, Dec 2002. (See: http://eprint.iacr.org/2002/044).
4. Y. Talwar, C.E. Veni Madhavan, N. Rajpal, "On the key expansion Mechanisms of the AES Ciphers: Rijndael, Serpent".
5. P. Chdowiec, K. Gaj, "Very compact FPGA implementation of the AES algorithm", Cryptographic hardware and embedded systems (CHES 2003), LNCS vol. 2779, pp. 319-333, Springer-Verlog, October 2003.
6. G. Rouvroy, F.X. Standaert, J.J. Quisquater, J.D. Legat, , Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications, Proceedings of the international conference on Information Technology: coding and computing 2004 (ITCC 2004), pp. 583-587, vol. 2, April 2004.
7. Tim Good and Mohammed Benaissa, "AES on FPGA from the Fastest to the Smallest", CHES 2005, LNCS 3659, pp. 427-440, 2005. Springer-Verlog Berlin Heidelberg 2005.
8. Y. Talwar, C.E. Veni Madhavan, Navin Rajpal, "On Partial Linearization of Byte Substitution Transformation of Rijndael-The AES". Journal of Computer Science 2(1): 48-52, 2006, ISSN1549-3636 © 2006 Science Publications.
9. Swinder Kaur and Prof. Renu Vig, "Efficient Implementation of AES Algorithm in FPGA Devices". International Conference on Computational intelligence and Multimedia Applications 2007, DOI 10.1109/ICCIMA -2007.250, pages 179-187,0-7695-3050-8/07, IEEE-(2007) Volume2, pp 179-187.
10. J. Elbirt, W. Yip, B. Chatwynd and C. Paes, "An FPGA Implementation and performance Evaluation of the AES block cipher candidate algorithm analyst", Presented at Proc.3rd AES Conf. (AES). Available: http:// csrc.nist.gov/encryption/AES/round2/conf3/aes3paper.html.
11. Thulasimani L. and Madheswarn, "A Single Chip Design and Implementation of AES-128/192/256 Encryption Algorithms", International journal of Engineering Science and Technology (IJEST); ISSN: 0975-5462, Vol.2(5), 2010, 1052-1059.
12. M. McLoone and J. V. McCanny, "Rijndael FPGA implementation utilizing look-up tables" , in IEEE Workshop on Signal processing systems, Sept. 2001, pp. 349-360.
13. Amandeep Kaur, Puneet Bhardwaj and Naveen Kumar, "FPGA Implementation of Efficient Hardware for the Advanced Encryption Standard", in IJITEE; ISSN: 2278-3075, Volume-2, Issue-3, February 2013.

2.

Authors: A.E.Al-Salami

Paper Title: Quantifying Physical Parameters of Quaternary Glass with Composition Tellurium- Niobium - Zinc-Lithium Oxide

Abstract: In the present work the tellurite glass a function of alkali metals as network intermediate with composition 85TeO2/ 5Nb2O5/ 5ZnO/ 5Li2O in mol% were been prepared. These glasses contain Li2O can be promising used in optical devices because it has advantage optical properties compared with other tellurite glasses. The physical parameters of these glass studied with respect to values of density, □, molar volume, Vm, linear refractive indices, n0, nonlinear refractive index, n2, electronic polarizability, □m, molar refraction, Rm, metallization criterion, M (n0), and third order non-linear optical susceptibility, □(3),. The Sellmeier gap energy, Es, and dispersion energy, Ed, were calculated besides the theoretical third order of nonlinear optical susceptibility, □(3), calculated by used Lines model. Measure the thermal stability and the glass transition temperature by differential thermal analysis (Shimadzu DTA 50) which can be determine the glass transition temperature, Tg, onset crystallization temperature, Tc, and melting temperature, Tm. These glass have values as; □= 5.231 gm□cm-3, Vm= 28.75 cm-3, n0= 2.2228 at 435.84 nm, □m= 6.478Å3 and Rm=16.024 mol-1□cm3 at 435.84nm. and Es = 6.54 eV, Ed= 20.65 eV.

Keywords: Oxide glass; linear refractive index; dispersion energy.

References:

1. A. Assadi, K. Damak, R. Lachheb, A. Herrmann, E. Yousef, C. Russel, R. Maalej "SPECTROSCOPIC AND LUMINESCENCE CHARACTERISTICS OF ERBIUM DOPED TNZL GLASS FOR LASING MATERIALS" ,J. Alloys& Compounds 620 (2015), 129–136.
2. E Yousef, A E Al-Salami, A Salem, and E R, Shaaban" Optical and kinetics studies of titanium- zinc-niobium-tellurim oxides glass" Phys. Scr. 83 (2011) 01570
3. El Sayed Yousef, A. E. Al-salami, E. R. Shaaban "A TEM study and non-isothermal crystallization kinetic of tellurite glass-ceramics," J. Material Science 45 (2010) 5929–5936.
4. El Sayed Yousef, Mario Horzel, Christian Russel "The effect of CdS addition on linear and non-linear refractive indices of glasses in the systemTeO2/Nb2O5/ZnO," J. Non-Cryst. Solids 354 (2008) 4675.
5. H. Takebe, S. Fujino, K. Morinaga "REFRACTIVE-INDEX DISPERSION OF TELLURITE GLASSES IN THE REGION FROM 0.40 TO 1.71 MM," J. Am. Ceram. Soc., 77[9] (1994) pp. 2455–2457.
6. M. Didomenico, S. H. Wemple "Oxygen-Octahedra Ferroelectrics. I. Theory of Electro-optical and Nonlinear optical Effects," J. Appl. Phys. 40 [2] 720 (1969) pp.720-734.
7. El Sayed Yousef, A E Al-Salami, Mario Hotzel "Optical and thermal characteristics of glasses based on TeO2," Bull. Mater. Sci., Vol. 35, No. 6, (2012) pp.961-967.

8. K. Fajans, N. Kreid "STABILITY OF LEAD GLASSES AND POLARIZATION OF IONS," J. Am. Ceram. Soc. 31 (1948) pp.105-114.
9. Kordes "Physikalisch-chemische Untersuchungen über den Feinbau von Gläsern. I. Mitteilung. Die olrefraktion binärer Phosphat-, Silikat- und Boratgläser ," Z. anorg. Allg. Chem. 241 (1939) pp.1-38.
10. W. A. Weyl, E. G. Marboe, "the Constitution of Glasses," Wiley/Interscience,1962, New York.
11. El Sayed Yousef, S. F. Mansour, M. Y. Hassan, A. M. Emara"Synthesis optical properties of novel TeO2 based glasses," J. of Optik 127 (2016) pp.8933-8939.
12. H. Burger, W. Vogel, V. Kozhukharov "IR transmission and properties of glasses in the TeO2−RnOm, RnXm, Rn(SO4)m, Rn(PO3)mandB2O3] systems," Infrared Phys. 25 (1995) pp.395-409.
13. Charles C. Wang, Empirical Relation between the Linear and the Third-Order Nonlinear Optical Susceptibilities "Phys. Rev. B 2 (1970) 2045.
14. V. Dimitrov, S. Sakka, "Linear and nonlinear optical properties of simple oxides. II," J. Appl. Phys. 79 (1996)1741-1745.
15. Vesselin Dimitrov, Takayuki Komatsu"Electronic polarizability, optical basicity and non-linear optical properties of oxide glasses," , J. Non-Cryst. Solids 249 (1999) pp.160-179.
16. S. H. Wample," Optical oscillator strengths and excitation energies in solids, liquids, and molecules" J. Chem. Phys. 67 (1977) 2151.
17. M. E. Lines, " Bond-orbital theory of linear and nonlinear electronic response in ionic crystals. II. Nonlinear response" Phys. Rev. B 41, 3383 – (1990).

3.

Authors: **Javed Ali**

Paper Title: **Superiority of Agile over Software Models**

Abstract: The Software Development Life Cycle (SDLC) is a structure imposed on the development of software product and also known as Software Development Processes. It is often considered as a subset of a system development life cycle. There are numerous SDLC models widely used for developing software. The SDLC model gives a theoretical guide line regarding development of the software. The every SDLC has its own benefits and drawbacks according to that we decide which models should be implemented under which conditions. The concept of system lifecycle models came into existence that emphasized on the need to follow some structured approach towards building new or improved system. In this paper, the comparative study made on standard life cycle models namely rapid application development, Agile Development Model, V-shaped model, spiral model, incremental model and waterfall model, prototype.

Keywords: Software Development, Life Cycle, Model, Agile Development, Extreme Programming, Dynamic, Adaptive.

References:

1. Agrawal, Ashish, Mohd Aurangzeb Atiq, and L. S. Maurya. "A Current Study on the Limitations of Agile Methods in Industry Using Secure Google Forms."Procedia Computer Science 78 (2016): 291-297.
2. Raj, Gaurav, Dheerendra Singh, and Ankur Bansal. "Analysis for security implementation in SDLC."
3. In Confluence The Next Generation Information Technology Summit (Confluence), 2014 5th International Conference-, pp. 221-226. IEEE, 2014.
4. Sharma, Anubha, Manoj Kumar, and Sonali Agarwal. "A Complete Survey on Software Architectural Styles and Patterns." Procedia Computer Science 70 (2015): 16-28.
5. Langer, Arthur M. "System Development Life Cycle (SDLC)." In Analysis and Design of Information Systems, pp. 10-20. Springer London, 2008.
6. Montini, Denis Ávila, Danilo Douradinho Fernandes, Francisco Supino Marcondes, Paulo Marcelo Tasinaffo, Italo Santiago Vega, and Luiz Alberto Vieira Dias. "Formal Approach Use to Choose a Software Manufactoring Cell's SDLC." In 2010 Seventh International Conference on Information Technology, pp. 1304-1305. IEEE, 2010.
7. Tohidi, Hamid. "The Role of Risk Management in IT systems of organizations." Procedia Computer Science 3 (2011): 881-887.
8. Kumar, Chandan, and Dilip Kumar Yadav. "A Probabilistic Software Risk Assessment and Estimation Model for Software Projects." Procedia Computer Science 54 (2015): 353-361.
9. Molokken-Ostvold et.al, "A comparison of software project overruns - flexible versus sequential development models", Volume 31, Issue 9, Page(s): 754 – 766, IEEE CNF, Sept.2005.
10. Niazi, Mahmood, Muhammad Ali Babar, and June M. Verner. "Software Process Improvement barriers: A cross-cultural comparison." Information and software technology 52, no. 11 (2010): 1204-1216.Dybå, Tore. "An empirical investigation of the key factors for success in software process improvement." Software Engineering, IEEE Transactions on31, no. 5 (2005): 410-424.
11. Liao, Li, Yuzhong Qu, and Hareton KN Leung. "A software process ontology and its application."(2003).
12. Laura C. Rodriguez Martinez, Manuel Mora, Francisco. Alvarez, "A Descriptive/Comparative Study of the Evolution of Process Models of Software Development Life Cycles", Proceedings of the 2009 Mexican International Conference on Computer Science IEEE Computer Society Washington, DC, USA, 2009.
13. Sharma, B.; Sharma. N, "Software Process Improvement: A Comparative Analysis of SPI models", Emerging Trends in Engineering and Technology (ICETET), 2009 2nd International Conference on,16-18, 2009, pp. 1019- 1024.
14. M. Davis, H. Bersoff, E. R. Comer, "A Strategy for Comparing Alternative Software Development Life Cycle Models", Journal IEEE Transactions on Software Engineering ,Vol. 14, Issue 10, 1988.
15. Maglyas, A.; Nikula, U.; Smolander, K.,"Comparison of two models of success prediction in software development projects", Software Engineering Conference (CEE-SECR), 2010 6th Central and Eastern European on 13-15 Oct. 2010, pp. 43-49.
16. Gaurav Kumar, Pradeep Kumar Bhatia," Impact of Agile Methodology on Software Development Process"," ISSN 2249- 6343International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 4",august 2012.
17. Guy Want, "Drowning in the Waterfall, The Benefits of Agile versus the Predominance of Waterfall "Software Engineering CS 390:", October 29, 2008.

14-19

4.

Authors: **Alyaseh Nagi, Issa Ali, Sedat Nazlibilek**

Paper Title: **Decentralized Control Based On Active Disturbance Rejection Controller: An Application Quadruple Tank System**

Abstract: This paper presents Decentralized Control for the Quadruple Tank System (QTS) Based on Active Disturbance Rejection Controller (ADRC). The most remarkable advantages of the proposed approach are that it is not depend on the accuracy of mathematical model of the plant along with its simple structure and the ability of strong disturbance rejection. Often, there are some difficulties in designing of suitable controller for Quadruple Tank System due to the interaction between the inputs and outputs of this system. With the proposed control method, the cross coupling within the system treated as a disturbance, which is estimated using extended state observer (ESO) and then actively rejected. The Quadruple Tank System is represented using set of nonlinear differential equations

20-25

and the ADRC controller is applied directly on the nonlinear model of the system. The effectiveness of the proposed approach is validated via simulation results obtained under MATLAB environment. The results show that the ADRC gives better results compared to nonlinear optimal control strategy.

Keywords: Active Disturbance Rejection Controller Decentralized Control, Quadruple Tank System, The Nonlinear Coupling.

References:

1. V. V. Kumar, V. Rao, and M. Chidambaram, "Centralized PI controllers for interacting multivariable processes by synthesis method," ISA transactions, vol. 51, pp. 400-409, 2012.
2. B. Reddy, M. Chidambaram, and D. M. Al-Gobaisi, "Design of centralized controllers for a MSF desalination plant," Desalination, vol. 113, pp. 27-38, 1997.
3. Y. Shen, Y. Sun, and W. Xu, "Centralized PI/PID controller design for multivariable processes," Industrial & Engineering Chemistry Research, vol. 53, pp. 10439-10447, 2014.
4. E. Davison, "Multivariable tuning regulators: the feedforward and robust control of a general servomechanism problem," IEEE Transactions on Automatic Control, vol. 21, pp. 35-47, 1976.
5. K. S. Manic, S. Devakumar, V. Vijayan, and V. Rajinikanth, "Design of Centralized PI Controller for Interacting Conical Tank System," Indian Journal of Science and Technology, vol. 9, 2016.
6. Q.-G. Wang, B. Zou, T.-H. Lee, and Q. Bi, "Auto-tuning of multivariable PID controllers from decentralized relay feedback," Automatica, vol. 33, pp. 319-330, 1997.
7. P. Nordfeldt and T. Hägglund, "Decoupler and PID controller design of TITO systems," Journal of Process Control, vol. 16, pp. 923-936, 2006.
8. B. Parvat and B. Patre, "Design of SMC with decoupler for multi-variable coupled tank process," in 2014 Annual IEEE India Conference (INDICON), 2014, pp. 1-5.
9. B. T. Jevtović and M. R. Mataušek, "PID controller design of TITO system based on ideal decoupler," Journal of Process Control, vol. 20, pp. 869-876, 2010.
10. V. Dhanraj and D. Nanjundappan, "Design of optimized PI controller with ideal decoupler for a nonlinear multivariable system using particle swarm optimization technique," Int J Innov Comput Inform Control, vol. 10, pp. 341-355, 2014.
11. D. Šiljak and A. Zečević, "Control of large-scale systems: Beyond decentralized feedback," Annual Reviews in Control, vol. 29, pp. 169-179, 2005.
12. C.-S. Tseng and B.-S. Chen, "H∞ decentralized fuzzy model reference tracking control design for nonlinear interconnected systems," IEEE Transactions on fuzzy systems, vol. 9, pp. 795-809, 2001.
13. D. A. Vijula and N. Devarajan, "Design of Decentralised PI Controller using Model Reference Adaptive Control for Quadruple Tank Process," International Journal of Engineering and Technology, vol. 5, pp. 1347-1356, 2013.
14. J. Han, "From PID to active disturbance rejection control," IEEE transactions on Industrial Electronics, vol. 56, pp. 900-906, 2009.
15. D. Sun, "Comments on active disturbance rejection control," IEEE Transactions on Industrial Electronics, vol. 6, pp. 3428-3429, 2007.
16. S. Li, X. Yang, and D. Yang, "Active disturbance rejection control for high pointing accuracy and rotation speed," Automatica, vol. 45, pp. 1854-1860, 2009.
17. Y. Xia, B. Liu, and M. Fu, "Active disturbance rejection control for power plant with a single loop," Asian Journal of Control, vol. 14, pp. 239-250, 2012.
18. H.-L. Xing, J.-H. Jeon, K. Park, and I.-K. Oh, "Active disturbance rejection control for precise position tracking of ionic polymer–metal composite actuators," IEEE/ASME Transactions on Mechatronics, vol. 18, pp. 86-95, 2013.
19. F. Ferrese, Q. Dong, S. Biswas, and J. Batcho, "Decentralized control of coupled nonlinear dynamic systems with application to quadruple-tank process," in IECON 2014-40th Annual Conference of the IEEE Industrial Electronics Society, 2014, pp. 3657-3661.
20. J. Ramos and P. L. dos Santos, "Mathematical modeling, system identification, and controller design of a two tank system," in Decision and Control, 2007 46th IEEE Conference on, 2007, pp. 2838-2843.
21. X. Zuo, "Liquid level control of water tank system based on improved polyclonal selection algorithm and RBF network," in Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, 2010, pp. V2-528-V2-532.
22. M. Przybyła, M. Kordasz, R. Madoński, P. Herman, and P. Sauer, "Active Disturbance Rejection Control of a 2DOF manipulator with significant modeling uncertainty," Bulletin of the Polish Academy of Sciences: Technical Sciences, vol. 60, pp. 509-520, 2012.
23. J. Dong, L. Sun, D. Li, K. Y. Lee, and Z. Wu, "Inverted decoupling based active disturbance rejection control for multivariable systems," in 2015 54th IEEE Conference on Decision and Control (CDC), 2015, pp. 7353-7358.
24. S. Li, J. Yang, W.-H. Chen, and X. Chen, Disturbance observer-based control: methods and applications: CRC press, 2014.