



**HAL**  
open science

# A New Joint Lossless Compression and Encryption Scheme Combining a Binary Arithmetic Coding With a Pseudo Random Bit Generator

Atef Masmoudi, William Puech, Mohamed Selim Bouhleb

► **To cite this version:**

Atef Masmoudi, William Puech, Mohamed Selim Bouhleb. A New Joint Lossless Compression and Encryption Scheme Combining a Binary Arithmetic Coding With a Pseudo Random Bit Generator. International Journal of Computer Science and Information Security, 2010, 8 (1), pp.170-175. lirmm-00485850

**HAL Id: lirmm-00485850**

**<https://hal-lirmm.ccsd.cnrs.fr/lirmm-00485850>**

Submitted on 21 May 2010

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

**IJCSIS Vol. 8 No. 1, April 2010**  
**ISSN 1947-5500**

**International Journal of  
Computer Science  
& Information Security**

**© IJCSIS PUBLICATION 2010**

## Editorial Message from Managing Editor

*International Journal of Computer Science and Information Security (IJCSIS) provides a major venue for rapid publication of high quality computer science research, including multimedia, information science, security, mobile & wireless network, data mining, software engineering and emerging technologies etc. IJCSIS has continued to make progress and has attracted the attention of researchers worldwide, as indicated by the increasing number of both submissions and published papers, and also from the web statistics.. It is included in major Indexing and Abstracting services.*

*We thank all those authors who contributed papers to the April 2010 issue and the reviewers, all of whom responded to a short and challenging timetable. We are committed to placing this journal at the forefront for the dissemination of novel and exciting research. We should like to remind all prospective authors that IJCSIS does not have a page restriction. We look forward to receiving your submissions and to receiving feedback.*

*IJCSIS April 2010 Issue (Vol. 8, No. 1) has an acceptance rate of 35%.*

*Special thanks to our technical sponsors for their valuable service.*

**Available at <http://sites.google.com/site/ijcsis/>**

IJCSIS Vol. 8, No. 1, April 2010 Edition

ISSN 1947-5500 © IJCSIS 2010, USA.

*Indexed by (among others):*



## IJCSIS EDITORIAL BOARD

**Dr. Gregorio Martinez Perez**

Associate Professor - Professor Titular de Universidad, University of Murcia (UMU), Spain

**Dr. M. Emre Celebi,**

Assistant Professor, Department of Computer Science, Louisiana State University in Shreveport, USA

**Dr. Yong Li**

School of Electronic and Information Engineering, Beijing Jiaotong University, P. R. China

**Prof. Hamid Reza Naji**

Department of Computer Engineering, Shahid Beheshti University, Tehran, Iran

**Dr. Sanjay Jasola**

Professor and Dean, School of Information and Communication Technology, Gautam Buddha University

**Dr Riktesh Srivastava**

Assistant Professor, Information Systems, Skyline University College, University City of Sharjah, Sharjah, PO 1797, UAE

**Dr. Siddhivinayak Kulkarni**

University of Ballarat, Ballarat, Victoria, Australia

**Professor (Dr) Mokhtar Beldjehem**

Sainte-Anne University, Halifax, NS, Canada

**Dr. Alex Pappachen James, (Research Fellow)**

Queensland Micro-nanotechnology center, Griffith University, Australia

## TABLE OF CONTENTS

### **1. Paper 29031048: Buffer Management Algorithm Design and Implementation Based on Network Processors (pp. 1-8)**

*Yechang Fang, Kang Yen, Dept. of Electrical and Computer Engineering, Florida International University, Miami, USA*

*Deng Pan, Zhuo Sun, School of Computing and Information Sciences, Florida International University, Miami, USA*

### **2. Paper 08031001: Multistage Hybrid Arabic/Indian Numeral OCR System (pp. 9-18)**

*Yasser M. Alginaih, Ph.D., P.Eng. IEEE Member, Dept. of Computer Science, Taibah University, Madinah, Kingdom of Saudi Arabia*

*Abdul Ahad Siddiqi, Ph.D., Member IEEE & PEC, Dept. of Computer Science, Taibah University, Madinah, Kingdom of Saudi Arabia*

### **3. Paper 30031056: Attribute Weighting with Adaptive NBTree for Reducing False Positives in Intrusion Detection (pp. 19-26)**

*Dewan Md. Farid, and Jerome Darmont, ERIC Laboratory, University Lumière Lyon 2, Bat L - 5 av. Pierre Mendes, France, 69676 BRON Cedex, France*

*Mohammad Zahidur Rahman, Department of Computer Science and Engineering, Jahangirnagar University, Dhaka – 1342, Bangladesh*

### **4. Paper 30031053: Improving Overhead Computation and pre-processing Time for Grid Scheduling System (pp. 27-34)**

*Asgarali Bouyer, Mohammad javad hoseyni, Department of Computer Science, Islamic Azad University-Miyandoab branch, Miyandoab, Iran*

*Abdul Hanan Abdullah, Faculty Of Computer Science And Information Systems, Universiti Teknologi Malaysia, Johor, Malaysia*

### **5. Paper 20031026: The New Embedded System Design Methodology For Improving Design Process Performance (pp. 35-43)**

*Maman Abdurohman, Informatics Faculty, Telecom Institute of Technology, Bandung, Indonesia*

*Kuspriyanto, STEI Faculty, Bandung Institute of Technology, Bandung, Indonesia*

*Sarwono Sutikno, STEI Faculty, Bandung Institute of Technology, Bandung, Indonesia*

*Arif Sasongko, STEI Faculty, Bandung Institute of Technology, Bandung, Indonesia*

### **6. Paper 30031060: Semi-Trusted Mixer Based Privacy Preserving Distributed Data Mining for Resource Constrained Devices (pp. 44-51)**

*Md. Golam Kaosar, School of Engineering and Science, Victoria University, Melbourne, Australia*

*Xun Yi, Associate Preofessor, School of Engineering and Science, Victoria University, Melbourne, Australia*

### **7. Paper 12031005: Adaptive Slot Allocation And Bandwidth Sharing For Prioritized Handoff Calls In Mobile Networks (pp. 52-57)**

*S. Malathy, Research Scholar, Anna University, Coimbatore*

*G. Sudha Sadhasivam, Professor, CSE Department, PSG College of Technology, Coimbatore.*

*K. Murugan, Lecturer, IT Department, Hindusthan Institute of Technology, Coimbatore*

*S. Lokesh, Lecturer, CSE Department, Hindusthan Institute of Technology, Coimbatore*

**8. Paper 12031009: An Efficient Vein Pattern-based Recognition System (pp. 58-63)**

*Mohit Soni, DFS, New Delhi- 110003, INDIA.*

*Sandesh Gupta, UIET, CSJMU, Kanpur-208014, INDIA.*

*M.S. Rao, DFS, New Delhi-110003, INDIA*

*Phalguni Gupta, Professor, IIT Kanpur, Kanpur-208016, INDIA.*

**9. Paper 15031013: Extending Logical Networking Concepts in Overlay Network-on-Chip Architectures (pp. 64-67)**

*Omar Tayan*

*College of Computer Science and Engineering, Department of Computer Science, Taibah University, Saudi Arabia, P.O. Box 30002*

**10. Paper 15031015: Effective Bandwidth Utilization in IEEE802.11 for VOIP (pp. 68-75)**

*S. Vijay Bhanu, Research Scholar, Anna University, Coimbatore, Tamilnadu, India, Pincode-641013.*

*Dr.RM.Chandrasekaran, Registrar, Anna University, Trichy, Tamilnadu, India, Pincode: 620024.*

*Dr. V. Balakrishnan, Research Co-Supervisor, Anna University, Coimbatore.*

**11. Paper 16021024: ECG Feature Extraction Techniques - A Survey Approach (pp. 76-80)**

*S. Karpagachelvi, Mother Teresa Women's University, Kodaikanal, Tamilnadu, India.*

*Dr. M.Arthanari, Tejaa Shakthi Institute of Technology for Women, Coimbatore- 641 659, Tamilnadu, India.*

*M. Sivakumar, Anna University – Coimbatore, Tamilnadu, India*

**12. Paper 18031017: Implementation of the Six Channel Redundancy to achieve fault tolerance in testing of satellites (pp. 81-85)**

*H S Aravinda \*, Dr H D Maheshappa\*\*, Dr Ranjan Moodithaya \*\*\**

*\* Department of Electronics and Communication, REVA ITM, Bangalore-64, Karnataka, India.*

*\*\* Director & Principal, East Point College of Engg, Bidarahalli, Bangalore-40, Karnataka, India.*

*\*\*\* Head, KTMD Division, National Aerospace Laboratories, Bangalore-17, Karnataka, India.*

**13. Paper 18031018: Performance Oriented Query Processing In GEO Based Location Search Engines (pp. 86-94)**

*Dr. M. Umamaheswari, Bharath University, Chennai-73, Tamil Nadu,India,*

*S. Sivasubramanian, Bharath University, Chennai-73,Tamil Nadu,India,*

**14. Paper 20031027: Tunable Multifunction Filter Using Current Conveyor (pp. 95-98)**

*Manish Kumar, Electronics and Communication, Engineering Department, Jaypee Institute of Information Technology, Noida, India*

*M.C. Srivastava, Electronics and Communication, Engineering Department, Jaypee Institute of Information Technology, Noida, India*

*Umesh Kumar, Electrical Engineering Department, Indian Institute of Technology, Delhi, India*

**15. Paper 17031042: Artificial Neural Network based Diagnostic Model For Causes of Success and Failures (pp. 95-105)**

*Bikrampal Kaur, Chandigarh Engineering College, Mohali, India*

*Dr. Himanshu Aggarwal, Punjabi University, Patiala-147002, India*

**16. Paper 28031045: Detecting Security threats in the Router using Computational Intelligence (pp. 106-111)**

*J. Visumathi, Research Scholar, Sathyabama University, Chennai-600 119*

*Dr. K. L. Shunmuganathan, Professor & Head, Department of CSE, R.M.K. Engineering College, Chennai-601 206*

**17. Paper 31031091: A Novel Algorithm for Informative Meta Similarity Clusters Using Minimum Spanning Tree (pp. 112-120)**

*S. John Peter, Department of Computer Science and Research Center, St. Xavier's College, Palayamkottai, Tamil Nadu, India*

*S. P. Victor, Department of Computer Science and Research Center, St. Xavier's College, Palayamkottai, Tamil Nadu, India*

**18. Paper 23031032: Adaptive Tuning Algorithm for Performance tuning of Database Management System (pp. 121-124)**

*S. F. Rodd, Department of Information Science and Engineering, KLS's Gogte Institute of Technology, Belgaum, INDIA*

*Dr. U. P. Kulkarni, Department of Computer Science and Engineering, SDM College of Engineering and Technology, Dharwad, INDIA*

**19. Paper 26031038: A Survey of Mobile WiMAX IEEE 802.16m Standard (pp. 125-131)**

*Mr. Jha Rakesh, Deptt. Of E & T.C., SVNIT, Surat, India*

*Mr. Wankhede Vishal A., Deptt. Of E & T.C., SVNIT, Surat, India*

*Prof. Dr. Upena Dalal, Deptt. Of E & T.C., SVNIT, Surat, India*

**20. Paper 27031040: An Analysis for Mining Imbalanced Datasets (pp. 132-137)**

*T. Deepa, Faculty of Computer Science Department, Sri Ramakrishna College of Arts and Science for Women, Coimbatore, Tamilnadu, India.*

*Dr. M. Punithavalli, Director & Head, Sri Ramakrishna College of Arts & Science for Women, Coimbatore, Tamil Nadu, India*

**21. Paper 27031039: QoS Routing For Mobile Adhoc Networks And Performance Analysis Using OLSR Protocol (pp. 138-150)**

*K.Oudidi, Si2M Laboratory, National School of Computer Science and Systems Analysis, Rabat, Morocco*

*A. Hajami, Si2M Laboratory, National School of Computer Science and Systems Analysis, Rabat, Morocco*

*M. Elkoutbi, Si2M Laboratory, National School of Computer Science and Systems Analysis, Rabat, Morocco*

**22. Paper 28031047: Design of Simple and Efficient Revocation List Distribution in Urban Areas for VANET's (pp. 151-155)**

*Ghassan Samara , National Advanced IPv6 Center, Universiti Sains Malaysia, Penang, Malaysia*

*Sureswaran Ramadas, National Advanced IPv6 Center, Universiti Sains Malaysia, Penang, Malaysia*

*Wafaa A.H. Al-Salihy, School of Computer Science, Universiti Sains Malaysia, Penang, Malaysia*

**23. Paper 28031044: Software Process Improvization Framework For Indian Small Scale Software Organizations Using Fuzzy Logic (pp. 156-162)**

*A. M. Kalpana, Research Scholar, Anna University Coimbatore, Tamilnadu, India*

*Dr. A. Ebenezer Jeyakumar, Director/Academics, SREC, Coimbatore, Tamilnadu, India*

**24. Paper 30031052: Urbanizing the Rural Agriculture - Knowledge Dissemination using Natural Language Processing (pp. 163-169)**

*Priyanka Vij (Author) Student, Computer Science Engg. Lingaya"s Institute of Mgt. & Tech, Faridabad, Haryana, India*

*Harsh Chaudhary (Author) Student, Computer Science Engg. Lingaya"s Institute of Mgt. & Tech, Faridabad, Haryana, India*

*Priyatosh Kashyap (Author) Student, Computer Science Engg. Lingaya"s Institute of Mgt. & Tech, Faridabad, Haryana, India*

**25. Paper 31031073: A New Joint Lossless Compression And Encryption Scheme Combining A Binary Arithmetic Coding With A Pseudo Random Bit Generator (pp. 170-175)**

*A. Masmoudi \*, W. Puech \*\*, And M. S. Bouhleb \**

*\* Research Unit: Sciences and Technologies of Image and Telecommunications, Higher Institute of Biotechnology, Sfax TUNISIA*

*\*\* Laboratory LIRMM, UMR 5506 CNRS University of Montpellier II, 161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE*

**26. Paper 15031012: A Collaborative Model for Data Privacy and its Legal Enforcement (pp. 176-182)**

*Manasdeep, MSCLIS, IIT Allahabad*

*Damneet Singh Jolly, MSCLIS, IIT Allahabad*

*Amit Kumar Singh, MSCLIS, IIT Allahabad*

*Kamleshwar Singh, MSCLIS, IIT Allahabad*

*Mr Ashish Srivastava, Faculty, MSCLIS, IIT Allahabad*

**27. Paper 12031010: A New Exam Management System Based on Semi-Automated Answer Checking System (pp. 183-189)**

*Arash Habibi Lashkari, Faculty of ICT, LIMKOKWING University of Creative Technology, CYBERJAYA, Selangor,*

*Dr. Edmund Ng Giap Weng, Faculty of Cognitive Sciences and Human Development, University Malaysia Sarawak (UNIMAS)*

*Behrang Parhizkar, Faculty of Information, Communication And Technology, LIMKOKWING University of Creative Technology, CYBERJAYA, Selangor, Malaysia*

*Siti Fazilah Shamsudin, Faculty of ICT, LIMKOKWING University of Creative Technology, CYBERJAYA, Selangor, Malaysia*

*Jawad Tayyub, Software Engineering With Multimedia, LIMKOKWING University of Creative Technology, CYBERJAYA, Selangor, Malaysia*

**28. Paper 30031064: Development of Multi-Agent System for Fire Accident Detection Using Gaia Methodology (pp. 190-194)**

*Gowri. R, Kailas. A, Jeyaprakash.R, Carani Anirudh*

*Department of Information Technology, Sri Manakula Vinayagar Engineering College, Puducherry – 605 107.*

**29. Paper 19031022: Computational Fault Diagnosis Technique for Analog Electronic Circuits using Markov Parameters (pp. 195-202)**

*V. Prasannamoorthy and N.Devarajan*

*Department of Electrical Engineering, Government College of Technology, Coimbatore, India*

**30. Paper 24031037: Applicability of Data Mining Techniques for Climate Prediction – A Survey Approach (pp. 203-206)**

*Dr. S. Santhosh Baboo, Reader, PG and Research department of Computer Science, Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai*  
*I. Kadar Shereef, Head, Department of Computer Applications, Sree Saraswathi Thyagaraja College, Pollachi*

**31. Paper 17021025: Appliance Mobile Positioning System (AMPS) (An Advanced mobile Application) (pp. 207-215)**

Arash Habibi Lashkari, Faculty of ICT, LIMKOKWING University of Creative Technology, CYBERJAYA, Selangor, Malaysia  
Edmund Ng Giap Weng, Faculty of Cognitive Sciences and Human Development, University Malaysia Sarawak (UNIMAS)  
Behrang Parhizkar, Faculty of ICT, LIMKOKWING University of Creative Technology, CYBERJAYA, Selangor, Malaysia  
Hameedur Rahman, Software Engineering with Multimedia, LIMKOKWING University of Creative Technology, CYBERJAYA, Selangor, Malaysia

**32. Paper 24031036: A Survey on Data Mining Techniques for Gene Selection and Cancer Classification (pp. 216-221)**

*Dr. S. Santhosh Baboo, Reader, PG and Research department of Computer Science, Dwaraka Doss Goverdhan Doss Vaishnav College, Chennai*  
*S. Sasikala, Head, Department of Computer Science, Sree Saraswathi Thyagaraja College, Pollachi*

**33. Paper 23031033: Non-Blind Image Watermarking Scheme using DWT-SVD Domain (pp. 222-228)**

*M. Devapriya, Asst.Professor, Dept of Computer Science, Government Arts College, Udumalpet.*  
*Dr. K. Ramar, Professor & HOD, Dept of CSE, National Engineering College, Kovilpatti -628 502.*

**34. Paper 31031074: Speech Segmentation Algorithm Based On Fuzzy Memberships (pp. 229-233)**

*Luis D. Huerta, Jose Antonio Huesca and Julio C. Contreras*  
*Departamento de Informática, Universidad del Istmo Campus Ixtepec, Ixtepec Oaxaca, México*

**35. Paper 30031058: How not to share a set of secrets (pp. 234-237)**

*K. R. Sahasranand, Nithin Nagaraj, Department of Electronics and Communication Engineering, Amrita Vishwa Vidyapeetham, Amritapuri Campus, Kollam-690525, Kerala, India.*  
*Rajan S., Department of Mathematics, Amrita Vishwa Vidyapeetham, Amritapuri Campus, Kollam-690525, Kerala, India.*

**36. Paper 30031057: Secure Framework for Mobile Devices to Access Grid Infrastructure (pp. 238-243)**

*Kashif Munir, Computer Science and Engineering Technology Unit King Fahd University of Petroleum and Minerals HBCC Campus, King Faisal Street, Hafr Al Batin 31991*  
*Lawan Ahmad Mohammad, Computer Science and Engineering Technology Unit King Fahd University of Petroleum and Minerals HBCC Campus, King Faisal Street, Hafr Al Batin 31991*

**37. Paper 31031076: DSP Specific Optimized Implementation of Viterbi Decoder (pp. 244-249)**

*Yame Asfia and Dr Muhamamd Younis Javed, Department of Computer Engg, College of Electrical and Mechanical Engg, NUST, Rawalpindi, Pakistan*

*Dr Muid-ur-Rahman Mufti, Department of Computer Engg, UET Taxila, Taxila, Pakistan*

**38. Paper 31031089: Approach towards analyzing motion of mobile nodes- A survey and graphical representation (pp. 250-253)**

*A. Kumar, Sir Padampat Singhania University, Udaipur , Rajasthan , India  
P.Chakrabarti, Sir Padampat Singhania University, Udaipur , Rajasthan , India  
P. Saini, Sir Padampat Singhania University, Udaipur , Rajasthan , India*

**39. Paper 31031092: Recognition of Printed Bangla Document from Textual Image Using Multi-Layer Perceptron (MLP) Neural Network (pp. 254-259)**

*Md. Musfique Anwar, Nasrin Sultana Shume, P. K. M. Moniruzzaman and Md. Al-Amin Bhuiyan  
Dept. of Computer Science & Engineering, Jahangirnagar University, Bangladesh*

**40. Paper 31031081: Application Of Fuzzy System In Segmentation Of MRI Brain Tumor (pp. 261-270)**

*Mrigank Rajya, Sonal Rewri, Swati Sheoran  
CSE, Lingaya's University, Limat, Faridabad India, New Delhi, India*

**41. Paper 30031059: E-Speed Governors For Public Transport Vehicles (pp. 270-274)**

*C. S. Sridhar, Dr. R. ShashiKumar, Dr. S. Madhava Kumar, Manjula Sridhar, Varun. D  
ECE dept, SJCIT, Chikkaballapur.*

**42. Paper 31031087: Inaccuracy Minimization by Partioning Fuzzy Data Sets - Validation of Analytical Methodology (pp. 275-280)**

*Arutchelvan. G, Department of Computer Science and Applications Adhiparasakthi College of Arts and Science G. B. Nagar, Kalavai , India  
Dr. Srivatsa S. K., Dept. of Electronics Engineering, Madras Institute of Technology, Anna University, Chennai, India  
Dr. Jagannathan. R, Vinayaka Mission University, Chennai, India*

**43. Paper 30031065: Selection of Architecture Styles using Analytic Network Process for the Optimization of Software Architecture (pp. 281-288)**

*K. Delhi Babu, S.V. University, Tirupati  
Dr. P. Govinda Rajulu, S.V. University, Tirupati  
Dr. A. Ramamohana Reddy, S.V. University, Tirupati  
Ms. A.N. Aruna Kumari, Sree Vidyanikethan Engg. College, Tirupati*

**44. Paper 27031041: Clustering Time Series Data Stream – A Literature Survey (pp. 289-294)**

*V.Kavitha, Computer Science Department, Sri Ramakrishna College of Arts and Science for Women, Coimbatore, Tamilnadu, India.  
M. Punithavalli, Sri Ramakrishna College of Arts & Science for Women, Coimbatore ,Tamil Nadu, India.*

**45. Paper 31031086: An Adaptive Power Efficient Packet Scheduling Algorithm for Wimax Networks (pp. 295-300)**

*R Murali Prasad, Department of Electronics and Communications, MLR Institute of technology, Hyderabad  
P. Satish Kumar, professor, Department of Electronics and Communications, CVR college of engineering, Hyderabad*

**46. Paper 30041037: Content Base Image Retrieval Using Phong Shading (pp. 301-306)**

*Uday Pratap Singh, LNCT, Bhopal (M.P) INDIA*  
*Sanjeev Jain, LNCT, Bhopal (M.P) INDIA*  
*Gulfishan Firdose Ahmed, LNCT, Bhopal (M.P) INDIA*

**47. Paper 31031090: The Algorithm Analysis of E-Commerce Security Issues for Online Payment Transaction System in Banking Technology (pp. 307-312)**

*Raju Barskar, MANIT Bhopal (M.P)*  
*Anjana Jayant Deen, CSE Department, UIT\_RGPV, Bhopal (M.P)*  
*Jyoti Bharti, IT Department, MANIT, Bhopal (M.P)*  
*Gulfishan Firdose Ahmed, LNCT, Bhopal (M.P)*

**48. Paper 28031046: Reduction in iron losses In Indirect Vector-Controlled IM Drive Using FLC (pp. 313-317)**

*Mr. C. Srisailam , Electrical Engineering Department, Jabalpur Engineering College, Jabalpur, Madhya Pradesh,*  
*Mr. Mukesh Tiwari, Electrical Engineering Department, Jabalpur Engineering College, Jabalpur, Madhya Pradesh,*  
*Dr. Anurag Trivedi, Electrical Engineering Department, Jabalpur Engineering College, Jabalpur, Madhya Pradesh*

**49. Paper 31031071: Bio-Authentication based Secure Transmission System using Steganography (pp. 318-324)**

*Najme Zehra, Assistant Professor, Computer Science Department, Indira Gandhi Institute of Technology, GGSIPU, Delhi.*  
*Mansi Sharma, Scholar, Indira Gandhi Institute of Technology, GGSIPU, Delhi.*  
*Somya Ahuja, Scholar, Indira Gandhi Institute of Technology, GGSIPU, Delhi.*  
*Shubha Bansal, Scholar, Indira Gandhi Institute of Technology, GGSIPU, Delhi.*

**50. Paper 31031068: Facial Recognition Technology: An analysis with scope in India (pp. 325-330)**

*Dr.S.B.Thorat, Director, Institute of Technology and Mgmt, Nanded, Dist. - Nanded. (MS), India*  
*S. K. Nayak, Head, Dept. of Computer Science, Bahirji Smarak Mahavidyalaya, Basmathnagar, Dist. - Hingoli. (MS), India*  
*Miss. Jyoti P Dandale, Lecturer, Institute of Technology and Mgmt, Nanded, Dist. - Nanded. (MS), India*

**51. Paper 31031069: Classification and Performance of AQM-Based Schemes for Congestion Avoidance (pp. 331-340)**

*K.Chitra Lecturer, Dept. of Computer Science D.J.Academy for Managerial Excellence Coimbatore, Tamil Nadu, India – 641 032*  
*Dr. G. Padamavathi Professor & Head, Dept. of Computer Science Avinashilingam University for Women, Coimbatore, Tamil Nadu, India – 641 043*

# A new joint lossless compression and encryption scheme combining a binary arithmetic coding with a pseudo random bit generator

A. MASMOUDI #<sup>1</sup>, W. PUECH \*<sup>2</sup>, M.S. BOUHLEL #<sup>3</sup>

# *Research Unit: Sciences and Technologies of Image and Telecommunications, Higher Institute of Biotechnology Sfax TUNISIA*

<sup>1</sup> atef.masmoudi@lirmm.fr

<sup>3</sup> medsalim.bouhlel@enis.rnu.tn

\* *Laboratory LIRMM, UMR 5506 CNRS University of Montpellier II  
161, rue Ada, 34392 MONTPELLIER CEDEX 05, FRANCE*

<sup>2</sup> william.puech@lirmm.fr

**Abstract**—In this paper, we propose a new scheme which performs both lossless compression and encryption of data. The lossless compression is based on the arithmetic coding (AC) and the encryption is based on a pseudo random bit generator (PRBG). Thus, the plaintext is compressed with a binary arithmetic coding (BAC) whose two mapping intervals are swapped randomly by using a PRBG. In this paper, we propose a PRBG based on the standard chaotic map and the Engel Continued Fraction (ECF) map to generate a keystream with both good chaotic and statistical properties. To be used in cryptography, a PRBG may need to meet stronger requirements than for other applications. In particular, various statistical tests can be applied to the outputs of such generators to conclude whether the generator produces a truly random sequence or not. The numerical simulation analysis indicates that the proposed compression and encryption scheme satisfies highly security with no loss of the BAC compression efficiency.

## I. INTRODUCTION

In recent years, a variety of lossless data compression methods have been proposed [4], [3], [23], [31]. All of these methods can not perform both lossless compression and encryption of data. This paper presents a new scheme which combines arithmetic coding (AC) with a pseudo random bit generator (PRBG) to perform both compression and encryption of data.

AC has been widely used as an efficient compression algorithm in the new standards such JBIG2, JPEG2000 and H.264/AVC. For some specific applications, AC is also considered as an encryption algorithm. In [5], Cleary *et al.* considered the AC as an encryption scheme and they demonstrated that it is vulnerable against chosen plaintext attack and known plaintext attack. In [8], Bergen *et al.* studied the data security provided by an adaptive arithmetic coding (AAC). The improved algorithm based on regular re-initialisation and adjustment of one of the model parameters provides significant data security, but is vulnerable to a chosen plaintext attack. In [27], Wen *et al.* designed the binary arithmetic coding (BAC) with key-based interval splitting. They proposed to use a key for splitting the interval associated with the symbol to be encoded. Thus, the traditional assumption in AC that a single contiguous interval is used for each symbol is not preserved. The repeated splitting at each encoding/decoding

step allowing both encryption and compression. In [12], Kim *et al.* demonstrated the insecurity of the interval splitting AC against a known plain-text attack and a chosen plain-text attack. They also provided an improved version called the secure AC by applying a series of permutations at the input symbol sequence and output codeword. It should be noticed that due to the permutations process, the scheme has a high complexity and it is difficult to extend the secure AC to the context-based AC that exploits the input symbol redundancy to encode messages. In [34], Zhou *et al.* demonstrated that the secure AC is vulnerable against a chosen cipher-text attack. The basic idea is to progressively design codewords input to the decoder, and establish the correspondance of the bit location before and after the codeword permutation step. In [35], Zhou *et al.* presented a new scheme for joint security and performance enhancement of secure AC. They proposed to incorporate the interval splitting AC scheme with the bit-wise XOR operation. This scheme can be extended to any adaptive and context-based AC due to the elimination of the input symbol permutation step. In addition, the implementation is lower complexity than the original secure AC. Zhou *et al.* also presented a selective encryption scheme with even lower complexity. In [6], Grangetto *et al.* proposed a novel multimedia security framework by means of AC. The scheme is based on a random organization of the encoding intervals using a secret key. This technique can be applied to any multimedia coder employing AC as entropy coding stage, including static, adaptive and context-based AC. They proposed an implementation for their scheme tailored to the JPEG2000 standard. Mi *et al.* [17] proposed a new chaotic encryption scheme based on randomized AC using the logistic map for pseudo random bit generator. However, the logistic map is weak in security because it does not satisfy uniform distribution property and it has a small key space with only one control parameter [1], [2].

In addition, chaotic systems have been used for several applications [14], [32], [29], [30], [33] and some of these novel chaotic systems have designed pseudo random bit generators (PRBG) for stream cipher applications [10], [20]. The chaotic systems used in cryptography generate

a keystream with good properties such as ergodicity, sensitivity to initial values and sensitivity to control parameters. However, some of them are not very suitable to be used in cryptography due to their density function which is not uniform distributed or due to their small key space. To be used in cryptography, a PRBG may need to meet stronger requirements than for other applications. In particular, various statistical tests [21], [16] can be applied to the outputs of such generators to conclude whether the generator produces a truly random sequence or not. The use of ECF-map increases the complexity of a cryptosystem based on only one chaotic system and thus makes difficult to extract information about it [20]. In addition, ECF-map conserves the cryptography properties of the chaotic system; like sensitivity to initial conditions and control parameters; non periodicity and randomness; and add interesting statistical properties such uniform distribution density function and zero co-correlation.

In this paper, we propose a new joint compression and encryption scheme based on AC and PRBG. The proposed PRBG is based on the use of the standard chaotic map coupled with the Engle Continued Fractions (ECF) map. The outputs of the standard map are used as the inputs of ECF-map. The standard map with good chaotic properties and the ECF-map which possesses good statistical properties motivate us to design a new PRBG for secure AC.

The rest of this paper is organized as follows. In Section 2, we briefly discuss the AC. Section 3 details the proposed PRBG which is based on the standard chaotic map and the engel continued fraction map. In Section 4, we describe the proposed algorithm for secure AC. In Section 5, we analyze the security of the proposed scheme and we discuss experiment results. Finally, conclusions of this paper will be discussed in Section 6.

## II. OVERVIEW OF ARITHMETIC CODING

AC [13], [28], [9], [18] is a statistical coder and is very efficient for data compression. In addition, AC has been widely used in many standards including JPEG2000, JBIG2 and H.264/AVC. The principle of AC is that it assigns one codeword to the entire input data symbols and this codeword is a real number in the interval  $[0, 1)$ . To calculate the appropriate codeword for input data symbols, the AC works with a modeler that estimates the probability of each symbol at the encoding/decoding process. The model used by AC can be either static or adaptive. Let  $S = \{s_1, \dots, s_n\}$  be an independent and identically distributed binary sequence of  $n$  random symbols. During the encoding process, we firstly estimate the probability of each symbol and we calculate the cumulative distribution vector (CDV) by assigning, for each symbol  $s_i$ , a subinterval with a size proportional to its probability in the interval  $[0, 1)$ . Next, for any new symbol  $s_i$  from the input sequence, we select the subinterval for  $s_i$  and we define it as the new current interval. We iterate this step until all input sequence has been processed and we finally generate the codeword that uniquely identifies the final interval. There are many types of AC. Thus, the binary arithmetic coding (BAC) is an important type of encoder due to its

ability to reduce the complexity created with the dynamic update of the CDV when we use an adaptive models. In addition, BAC has universal applications because data symbols which are putted out from any alphabet can be coded as a sequence of binary symbols. When we work with a binary source alphabet, the CDV is  $[0, p_0, 1]$ , with  $p_0$  the probability of the symbol "0". The interval  $[0, 1)$  is partitionned in two parts. In this case, the symbol "0" is represented by the range  $[0, p_0)$  and the symbol "1" is represented by the range  $[p_0, 1)$ . The Algorithms 1 and 2 illustrate the encoding and decoding procedures for the BAC.

---

### Algorithm 1 Binary encoder

---

```
Initialize  $base \leftarrow 0$ ,  $length \leftarrow 2^N - 1$ 
for  $i \leftarrow 1$  to  $n$  do
   $x \leftarrow length \times p(0)$ 
  if  $b_i = 0$  then
     $length \leftarrow x$ 
  else
     $init\_base \leftarrow base$ 
     $base \leftarrow base + x$ 
     $length \leftarrow length - x$ 
    if  $init\_base > base$  then
      propagate_carry()
    end if
  end if
if  $length < length\_min$  then
  renorm_enc_interval()
end if
end for
```

---

---

### Algorithm 2 Binary Decoder

---

```
Initialize  $base \leftarrow 0$ ,  $length \leftarrow 2^N - 1$ , code = input 4
bytes from compressed file
while Not end of compressed file do
   $x \leftarrow length \times p(0)$ 
  if  $code \geq x$  then
     $b_i \leftarrow 1$ 
  else
     $b_i \leftarrow 0$ 
  end if
  if  $b_i = 0$  then
     $length \leftarrow x$ 
  else
     $code \leftarrow code - x$ 
     $length \leftarrow length - x$ 
  end if
  if  $length < length\_min$  then
    renorm_dec_interval()
  end if
  output  $b_i$ 
end while
```

---

## III. PSEUDO RANDOM BITS GENERATED FROM THE STANDARD CHAOTIC MAP AND THE ECF-MAP

In this section, we describe the process of the proposed PRBG. In this PRBG, we suggest to use the standard chaotic map which is defined by:

$$\begin{cases} x_j = x_{j-1} + p_0 \times \sin(y_{j-1}) \\ y_j = y_{j-1} + x_j \end{cases}, \quad (1)$$

where  $x_j$  and  $y_j$  are taken modulo  $2\pi$ . The secret key in the proposed PRBG is a set of three floating point numbers and one integer  $(x_0, y_0, p_0, N_0)$ , where  $\{x_0, y_0\} \in [0, 2\pi)$  is the initial values set,  $p_0$  is the control parameter which can have any real value greater than 18.0 and  $N_0$  is the number of initial iterations of the standard chaotic map [19]. The standard map has good chaotic properties and a large key space of the order 157 bits [19] with an accuracy of  $10^{-14}$ . This key space is sufficient enough to resist the brute-force attack. However, the standard chaotic map generates a sequence with non uniform density function. The experimental results presented in Table I, show that sequences generated from standard chaotic map failed some tests of the NIST statistical test suite [21] and these sequences are not good enough to be used in cryptographic applications. It seems a good idea to transform the chaotic sequence generated from the standard chaotic map to a new sequence which satisfies uniform distribution property and have many important characteristics of cryptography such as zero co-correlation, randomness and ideal nonlinearity. In [7], a new nonlinear dynamical system has been proposed which called Engel Continued Fraction map.

The Engel continued fraction (ECF) map  $T_E : [0, 1] \rightarrow [0, 1)$  is given by:

$$T_E(x) = \begin{cases} \frac{1}{\lfloor \frac{1}{x} \rfloor} (\frac{1}{x} - \lfloor \frac{1}{x} \rfloor) & \text{if } x \neq 0 \\ 0 & \text{if } x = 0. \end{cases} \quad (2)$$

For any  $x \in [0, 1)$ , the ECF-map generates a new and unique continued fraction expansion [15], [22], [25], [24], [11] of  $x$  of the form:

$$x = \frac{1}{b_1 + \frac{b_1}{b_2 + \frac{b_1}{b_3 + \dots + \frac{b_{n-1}}{b_n + \dots}}}}}, \quad b_n \in \mathbb{N}, \quad b_n \leq b_{n+1} \quad (3)$$

Let  $x \in [0, 1)$ , and define:

$$\begin{aligned} b_1 &= b_1(x) = \lfloor \frac{1}{x} \rfloor \\ b_n &= b_n(x) = b_1(T_E^{n-1}(x)), \quad n \geq 2, \quad T_E^{n-1}(x) \neq 0, \end{aligned} \quad (4)$$

where  $T_E^0(x) = x$  and  $T_E^n(x) = T_E(T_E^{n-1}(x))$  for  $n \geq 1$ . From definition of  $T_E$  it follows that:

$$\begin{aligned} x &= \frac{1}{b_1 + b_1 T_E(x)} \\ &= \frac{1}{b_1 + \frac{b_1}{b_2 + \frac{b_1}{b_3 + \dots + \frac{b_{n-1}}{b_n + b_n T_E^n(x)}}}}}. \end{aligned} \quad (5)$$

The method used for generating the ECF-continued fraction expansion of  $x$  is described in Algorithm 3.

From the theorem presented in [7], if we let  $x \in [0, 1)$ , then  $x$  has a finite ECF-expansion (i.e.,  $T_E^n(x) = 0$  for some  $n \geq 1$ ) if and only if  $x \in \mathbb{Q}$ . Thus, all floating number has a unique and finite ECF-expansion. Note that, we paid most attention to the following sequence:

---

### Algorithm 3 ECF expansion

---

```

Initialize  $x_0 \leftarrow x, i \leftarrow 0$ 
while  $x_i \neq 0$  do
     $i \leftarrow i + 1$ 
     $b_i \leftarrow \lfloor \frac{1}{x_{i-1}} \rfloor$ 
     $x_i \leftarrow \frac{1}{\lfloor \frac{1}{x_{i-1}} \rfloor} (\frac{1}{x_{i-1}} - \lfloor \frac{1}{x_{i-1}} \rfloor)$ 
end while

```

---

$$Z_n(x) = b_n(x)T_E^n(x), \quad n \geq 1. \quad (6)$$

The sequence  $\{Z_i(x)\}_{i=1}^n$  is in  $[0, 1)$  and uniformly distributed for almost all points  $x$  (for a proof see [7]). So, the ECF-map generates a random and unpredictable sequence  $\{Z_i(x)\}_{i=1}^n$  with a uniform distribution. These properties, which are very useful in cryptography, motivate us to use ECF-map in our PRBG.

The use of the standard chaotic map make the output very sensitive to the input and in our PRBG, the outputs of this chaotic map are used as the input to the ECF-map for generating sequences with desirable chaotic and statistical properties.

In the following paragraph, we give the detailed procedure to generate pseudo random binary sequences using the standard and ECF maps.

We define a function  $G : [0, 1) \rightarrow [0, 1)$  such that:

$$G(x_i) = \sum_j Z_j(x_i) - \lfloor \sum_j Z_j(x_i) \rfloor, \quad (7)$$

where  $\{Z_j\}$  is the set calculated according to (6) using ECF-map. In addition, assume that we have defined a function  $F : [0, 1) \rightarrow \{0, 1\}$  that converts the real number  $x_i$  to a discrete bit symbol as follows:

$$F(x_i) = \begin{cases} 0 & \text{if } x_i < 0.5 \\ 1 & \text{otherwise} \end{cases}. \quad (8)$$

We propose to use the 2-D standard map, with  $\{x_0, y_0\}$  the initial values and  $p_0$  the control parameter of the chaotic map. The majority of cryptosystems with keystreams independent of plaintexts are vulnerable under known plaintext attacks [26]. Thus, to enhance the security of our encryption method, we propose to use the plaintext when producing keystreams. In our scheme, we firstly iterate the chaotic map  $N_0$  times and the operation procedures of the proposed PRBG are described as follows:

- **Step 1:** The standard map is iterated continuously. For the  $j$ th iteration, the output of the standard map is a new set  $\{x_j, y_j\}$ .
- **Step 2:** Assuming that the plaintext is a binary sequence  $B = b_1 \dots b_n$ . For the  $j$ th bit of the plaintext we calculate  $S_j$  the decimal representation of  $b_{j-8} \dots b_{j-1}$ . Note that for the first 8 bits of the plaintext,  $S_j$  equals to a secret value  $S_0$ . In addition, the standard map generates a set  $\{x_j, y_j\} \in [0, 2\pi)$ . So we propose to calculate the set  $\{a_j\}_{j=1}^n$  using the relation:

$$a_j = (x_j + y_j + \frac{S_j}{256}) - \lfloor (x_j + y_j + \frac{S_j}{256}) \rfloor. \quad (9)$$

- **Step 3:** Finally, the sequence  $K^n = \{k_j\}_{j=1}^n$  represents the random binary sequence and it is generated by:

$$k_j = F(G(a_j)). \quad (10)$$

The standard and ECF maps are iterated until the generation of a keystream with length  $n$ . In order to generate the random binary sequence  $\{k_j\}_{j=1}^n$ , an initial sequence  $\{a_j\}_{j=1}^n$  has to be created using the standard map. To test the randomness of the sequence generated by using the standard map, we propose to calculate the sequence  $\{M_j\}_{j=1}^n$  as follows:  $M_j = F(a_j)$  for  $1 \leq j \leq n$ . From a cryptographic point of view, the sequence  $\{M_j\}_{j=1}^n$  is not good enough for designing a PRBG because it does not pass all statistical tests designed by the NIST [21]. Therefore, we propose to use the ECF-map to convert the generated sequence  $\{a_j\}_{j=1}^n$  to a binary sequence  $\{k_j\}_{j=1}^n$  of the same length by applying (10). Table I shows the passing rate of the sequences without and with using ECF-map. A noticeable improvement is observed after mixing standard map with the ECF-map and all the tests are passed. Figures 1 and 2 present respectively the chaotic trajectory and the distribution function of the proposed PRBG for a keystream of length 10,000 bits generated with a random encryption key. In these two figures, we have supposed that the keystream acts as byte, so the range of the keystream is 0 – 255.

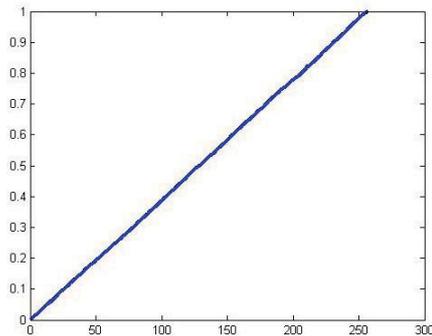


Fig. 1. Distribution function of the generated keystream by using our PRBG.

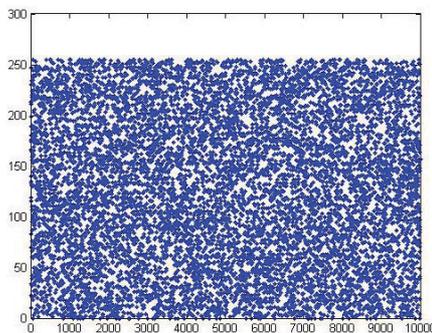


Fig. 2. The uniform property of the generated keystream by using our PRBG

#### IV. THE PROPOSED COMPRESSION AND ENCRYPTION SCHEME

We assume that the plaintext is a binary sequence  $B = b_1 \dots b_n$ . Let  $p_0$  the probability of symbol "0" and

$p_1$  the probability of symbol "1". We propose to use the keystream  $K^n = \{k_j\}_{j=1}^n$  generated from our PRBG to randomly exchange the two intervals of the CDV used in BAC encoding/decoding process. Thus, before encoding the bit  $b_j$  of the plaintext  $B$ , we propose to generate the  $j$ th key  $k_j$  using our PRBG. In the encryption and decryption algorithms, we suggest to use two variables called *lower* and *upper* which initially equal to 0 and 1 respectively, and the CDV is  $[0, p_0, 1]$ . If the generated key  $k_j$  equals to 1, then these two variables are permuted and the CDV becomes  $[0, p_1, 1]$ . So, we only suggest to permute the probabilities  $p_0$  and  $p_1$  in the CDV according to the generated key  $k_j$ . The encryption and decryption procedures are illustrated in Algorithms 4 and 5 respectively. The proposed scheme leads to make BAC performing both lossless compression and encryption simultaneously. In addition, AC is very sensitive to errors in the compressed data, and this undesired property ameliorates the security of the proposed method. The cryptographic properties of the proposed PRBG lead to perform maximum randomization in the swapping intervals process. The decryption process is similar to the encryption one. It should be noted that the proposed scheme conserves the compression efficiency of the BAC because we use the same probabilities when encoding the binary symbols without and with the permutation process. The most advantage of the work presented in this paper is the use of the chaos theory with the use of the ECF-map into arithmetic coding to provide a new scheme which performs both compression and encryption of data.

---

#### Algorithm 4 Encryption algorithm

---

```

Initialize  $base \leftarrow 0$ ,  $length \leftarrow 2^N - 1$ ,  $lower \leftarrow 0$ ,
 $upper \leftarrow 1$ ,
for  $i \leftarrow 1$  to  $n$  do
    generate  $k_i$  using the PRBG
    if  $K_i = 1$  then
         $permute(lower, upper)$ 
    end if
     $x \leftarrow length \times p(lower)$ 
    if  $b_i = lower$  then
         $length \leftarrow x$ 
    else
         $init\_base \leftarrow base$ 
         $base \leftarrow base + x$ 
         $length \leftarrow length - x$ 
        if  $init\_base > base$  then
             $propagate\_carry()$ 
        end if
    end if
    if  $length < length\_min$  then
         $renorm\_enc\_interval()$ 
    end if
end for

```

---

#### V. EXPERIMENT RESULTS AND SECURITY ANALYSIS

The BAC implementation used during the experiment analysis was downloaded from the website (<http://www.cipr.rpi.edu/~said/fastac.html>) and it was implemented using C++. In this paper, we propose to analyze

Test No.	Test Name	$x_0 = 3.59587469543$ $y_0 = 0.8512974635$ $p_0 = 120.9625487136$ $N_0 = 250$		$x_0 = 5.02548745491$ $y_0 = 2.9654128766$ $p_0 = 100.6$ $N_0 = 250$	
		$\{k_j\}_{j=1}^N$	$\{a_j\}_{j=1}^N$	$\{k_j\}_{j=1}^N$	$\{a_j\}_{j=1}^N$
1	FT	0.950563	0.000000	0.571394	0.000000
2	BFT (m = 128)	0.487702	0.004997	0.606546	0.025579
3	RT	0.852448	0.000000	0.588039	0.000000
4	LROT	0.909896	0.217013	0.676629	0.419327
5	MRT	0.931527	0.406179	0.104819	0.760720
6	SPT	0.760384	0.417304	0.067271	0.019833
7	NOTMT (m = 9, B = 000000001)	0.976154	0.004070	0.285350	0.000407
8	OTMT (m = 9, B = 111111111)	0.528047	0.000343	0.509185	0.198951
9	MUST (L=7, Q= 1280)	0.189804	0.026644	0.087637	0.296153
10	LZT	0.537151	0.234318	0.061457	0.002342
11	LCT (M = 500)	0.482937	0.275970	0.685647	0.829220
12	ST (m = 16)	0.442602	0.115116	0.252451	0.952714
13	AET	0.182287	0.000000	0.784454	0.000000
14	CST (Forward)	0.837613	0.000000	0.606517	0.000000
	CST(Reverse)	0.801266	0.000000	0.223216	0.000000
15	RET (x = +1)	0.938621	0.000000	0.403319	0.000000
16	REVT (x = -1)	0.241429	0.000000	0.764309	0.000000

TABLE I  
STATISTICAL TESTS ON THE SEQUENCES  $\{k_j\}_{j=1}^n$  AND  $\{M_j\}_{j=1}^n$  WITH DIFFERENT KEYS.

Lena bit plane $512 \times 512$	Static model		Adaptive model	
	Traditional AC	Our method	Traditional AC	Our method
Bit plane 8	32780	32780	27622	27622
Bit plane 7	32182	32182	30085	30085
Bit plane 6	32786	32786	31151	31151
Bit plane 5	32790	32790	32295	32295

TABLE II  
THE COMPRESSION EFFICIENCY (IN BYTE) OF BIT PLANE WITH DIFFERENT INFORMATION ENTROPY.

**Algorithm 5** Decryption algorithm

```

Initialize  $base \leftarrow 0$ ,  $length \leftarrow 2^N - 1$ , code = input 4
bytes from compressed file
while Not end of compressed file do
    generate  $k_i$  using the PRBG
    if  $K_i = 1$  then
        permute(lower, upper)
    end if
     $x \leftarrow length \times p(lower)$ 
    if code  $\geq x$  then
         $b_i \leftarrow upper$ 
        code  $\leftarrow code - x$ 
        length  $\leftarrow length - x$ 
    else
         $b_i \leftarrow lower$ 
        length  $\leftarrow x$ 
    end if
    if length < length_min then
        renorm_dec_interval()
    end if
    output  $b_i$ 
end while

```

Image size in pixels	Total elapsed time(s) using our method	
	in static model	in adaptive model
$256 \times 256$	2.30	3.00
$512 \times 512$	9.23	12.00
$1024 \times 1024$	34.30	45.50

TABLE III  
THE COMPRESSION AND ENCRYPTION SPEEDS OF OUR METHOD IN BOTH STATIC AND ADAPTIVE MODEL.

adaptive model. From Table II, the obtained bytes using both static and adaptive model are the same with and without using the encryption process. Thus, our proposed scheme conserves the compression efficiency.

There is an other important issue on a compression and encryption scheme which is the running speed. The analysis has been done using a machine with Intel core 2 Duo 2.93 GHZ CPU and 2 GB RAM running on Windows XP Professional Edition. The execution times of our method for images with different size are shown in Table III.

The proposed compression and encryption scheme is based on a BAC whose two mapping intervals are exchanged randomly by using a PRBG. This scheme is sensitive to both plaintext and key. As shown in Figure 3, the ciphertext has uniform distribution for both on static model and adaptive model. Therefore, the proposed scheme does not provide any clue to employ any statistical attack on the ciphertext.

our method in multimedia application and especially to each binary bit plane of the gray-scale images of different size with 8-bits per pixel. Table II shows the compression results of the Lena binary bit plane images for both traditional BAC and our approach in static model and

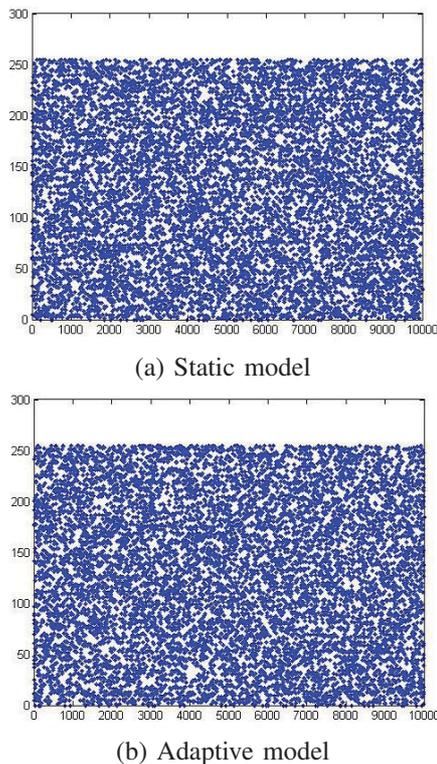


Fig. 3. The uniform property of the ciphertext for the first 10,000 bits of the encrypted Lena in (a) Static model and (b) Adaptive model.

## VI. CONCLUSIONS

In this paper, we proposed a new scheme which combines BAC with a PRBG to perform both lossless compression and encryption of data. In our scheme, we exploit both the efficiency of the BAC in lossless data compression and the advantages of chaos theory in data encryption to provide a scheme which can be very useful in many applications such as multimedia applications and medical imaging.

## REFERENCES

- [1] G. Alvarez, F. Montoya, M. Romera, and G. Pastor. Cryptanalysis of a Discrete Chaotic Cryptosystem Using External Key. *Physics Letters*, 9:319–334, 2003.
- [2] G. A. Alvarez and L. B. Shujun. Cryptanalyzing a Nonlinear Chaotic Algorithm (NCA) for Image Encryption. *Communications in Nonlinear Science and Numerical Simulation*, 14(11):3743–3749, 2009.
- [3] B. Carpentieri, M. J. Weinberger, and G. Seroussi. Lossless Compression of Continuous-Tone Images. *Proceedings of the IEEE*, 88(11):1797–1809, November 2000.
- [4] T. J. Chuang and J. C. Lin. A New Algorithm for Lossless Still Image Compression. *Pattern Recognition*, 31(9):1343–1352, September 1998.
- [5] J. Cleary, S. Irvine, and I. Rinsma-Melchert. On the Insecurity of Arithmetic Coding. *Computers and Security*, 14:167–180, 1995.
- [6] M. Grangetto, E. Magli, and G. Olmo. Multimedia Selective Encryption by Means of Randomized Arithmetic Coding. *IEEE Transactions on Multimedia*, 8(5):905–917, October 2006.
- [7] Y. Hartono, C. Kraaikamp, and F. Schweiger. Algebraic and Ergodic Properties of a New Continued Fraction Algorithm with Non-Decreasing Partial Quotients. *Journal de théorie des nombres de Bordeaux*, 14(2):497–516, 2002.
- [8] A. B. Helen and M. H. James. A chosen plaintext attack on an adaptive arithmetic coding compression algorithm. *Computers and Security*, 12:157–167, 1993.
- [9] P. G. Howard and J. S. Vitter. Arithmetic Coding for Data Compression. *Proceedings of the IEEE*, 82(6):857–865, Jun. 1994.
- [10] A. Kanso and N. Smaoui. Logistic Chaotic Maps for Binary Numbers Generations. *Chaos, Solitons and Fractals*, 40:2557–2568, 2009.
- [11] A. Y. Khintchin. Continued Fractions. *Noordhoff, Groningen*, 1963.
- [12] H. Kim, J. Wen, and J. Villasenor. Secure Arithmetic Coding. *IEEE Trans Signal Processing*, 55(5):2263–2272, 2007.
- [13] G. G. Langdon. An Introduction to Arithmetic Coding. *IBM Journal of Research and Development*, 28(2), Mar. 1984.
- [14] S. Li and X. Mou. Improving Security of a Chaotic Encryption Approach. *Physics Letters A*, 290(3-4):127–133, 2001.
- [15] L. Lorentzen and H. Waadeland. Continued Fractions with Applications. *North Holland*, 1992.
- [16] G. Marsaglia. DIEHARD: A Battery of Tests of Randomness. <http://stat.fsu.edu/geo/diehard.html>, 1997.
- [17] B. Mi, X. Liao, and Y. Chen. A Novel Chaotic Encryption Scheme Based on Arithmetic Coding. *Chaos, Solitons and Fractals*, 38:1523–1531, 2008.
- [18] A. Moffat, R. M. Neal, and I. H. Witten. Arithmetic Coding Revisited. *ACM Transactions on Information Systems*, 16(3):256–294, Jul. 1998.
- [19] V. Patidar, N. K. Parekk, and K. K. Sud. A New Substitution-Diffusion Based Image Cipher Using Chaotic Standard and Logistic Maps. *Communications in Nonlinear Science and Numerical Simulation*, 14:3056–3075, 2009.
- [20] V. Patidar and K. K. Sud. A Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing. *Electronic Journal of Theoretical Physics*, 6(20):327–344, 2009.
- [21] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. Statistical Test Suite for Random and Pseudo Random Number Generators for Cryptographic Applications. *NIST special publication 800-22 Revision 1*, 2008.
- [22] R. B. Seidensticker. Continued Fractions for High-Speed and High-Accuracy Computer Arithmetic. in *Proc. 6th IEEE Symp. Comput. Arithmetic*, 1983.
- [23] S. Sudharsanan and P. Sriram. Block-based Adaptive Lossless Image Coder. In *Proc. IEEE Int. Conf. on Image Processing, Vancouver, BC, Canada*, pages 120–123, 2000.
- [24] J. Vuillemin. Exact Real Computer Arithmetic with Continued Fractions. *INRIA Report 760. Le Chesnay, France: INRIA*, NOV. 1987.
- [25] H. S. Wall. Analytic Theory of Continued Fractions. *Chelsea*, 1973.
- [26] J. Wei, X. F. Liao, K. W. Wong, and T. Zhou. Cryptanalysis of Cryptosystem Using Multiple one-Dimensional Chaotic Maps. *Communications in Nonlinear Science and Numerical Simulation*, 12:814–22, 2007.
- [27] J.G. Wen, H. Kim, and J.D. Vilasenor. Binary Arithmetic Coding Using Key-Based Interval Splitting. *IEEE Signal Process Lett*, 13(2):69–72, 2006.
- [28] I. H. Witten, R. M. Neal, and J. G. Cleary. Arithmetic Coding for Data Compression. *Communications of the ACM*, 30(6):520–540, Jun. 1987.
- [29] K. W. Wong, B. S. H. Kwoka, and C. H. Yuena. An Efficient Diffusion Approach for Chaos-Based Image Encryption. *Chaos, Solitons and Fractals*, 41(5):2652–2663, 2008.
- [30] X. G. Wu, H. P. Hu B. L., and Zhang. Analyzing and Improving a Chaotic Encryption Method. *Chaos, Solitons and Fractals*, 22(2):367–373, 2004.
- [31] W. Xiaolin. An Algorithmic Study on Lossless Image Compression. In *Data Compression Conference*, pages 150–159. IEEE Computer Society Press, 1996.
- [32] T. Yang. A Survey of Chaotic Secure Communication Systems. *Journal of Computational Cognition*, 2(2):81–130, 2004.
- [33] L. Zhang, X. Liao, and X. Wang. An Image Encryption Approach Based on Chaotic Maps. *Chaos, Solitons and Fractals*, 24(3):759–765, 2005.
- [34] J. Zhou, O. C. Au, X. Fan, and P. H. W. Wong. Joint security and performance enhancement for secure arithmetic coding. *ICIP*, pages 3120–3123, 2008.
- [35] J. Zhou, O. C. Au, and P. H. Wong. Adaptive Chosen-Ciphertext Attack on Secure Arithmetic Coding. *IEEE Trans Signal Processing*, Feb. 2008.