Volume 35, Number 2, March 2009

ISSN 0045-7906

ELSEVIER

Computers and Electrical Engineering

AN INTERNATIONAL JOURNAL

Editor-in-Chief: **Mo Jamshidi**

Special Issue
Circuits and Systems for Real-Time Security and Copyright Protection of Multimedia

Guest Editors: **Saraju P. Mohanty**
Nasir Memon
Karam S. Chatha

http://www.elsevier.com/locate/compeleceng

Available online at

ScienceDirect

www.sciencedirect.com

Guest Editorial

Circuits and Systems for Real-Time Security and Copyright Protection of Multimedia

1. Introduction

Following the explosive growth of the Internet, concerns about protection and enforcement of IP rights of the digital content have been mounting. Unauthorized replication and manipulation of digital content is relatively easy and can be achieved with inexpensive tools. Consequently, motion picture and audio industry lose several billions dollars every year. DRM (Digital Rights Management) systems are essential for establishing ownership rights, tracking usage, ensuring authorized access, preventing illegal replication, and facilitating content authentication [1, 2]. Such DRM systems would be developed by exploiting various technologies such as encryption, watermarking, steganography, scrambling, digital certificates, secure communication protocols, fingerprinting, and hashing.

In the past decade significant research progress has been made to develop DRM techniques that primarily work offline [3, 4]. In the existing schemes watermarks are first inserted in the multimedia data before the watermarked images or video are made available to the user. There is a time gap between data capture and transmission to accommodate processing time for DRM. This approach works well for offline scenario, for example, in digital cinema and digital library, etc. However, the existing algorithms, approaches, and systems are computationally intensive and are not suitable for real-time applications.

In the case of emerging applications such as, digital television broadcasting, internet protocol television (IP-TV) [5, 6], video on demand, pay-TV, electronic passport (e-passport), credit cards, personal identity cards, driving licenses, etc [7, 8] security and copyright protection mechanisms have to work in real-time. Consequently, appliances like digital still camera, digital motion camera, network processor, mobile phones, video phones, graphics processing units, DVD players, etc. need to be equipped with suitable infrastructure for real-time DRM. In these situations, software only solutions may not be adequate to provide desired performance. Rather hardware assisted solutions are needed. In addition to real-time performance, the additional hardware must satisfy several desirable characteristics including easy integration with existing multimedia system, low power consumption, higher reliability and availability compared to software, and lower cost compared to software.

In order to address this important problem, multi-faceted research is required in (and not necessarily limited to) the following areas:

- Integrated circuits for real-time DRM systems.
- Operating-system and (micro) architecture-level support for security and copyright protection.
- Approaches for integrating security and copyright protection mechanisms in embedded architectures.
- Developing next generation System-on-Chip (SoC) based solutions with DRM technology for cameras, mobile phones, and network processors.
- Building media processors, graphics processing units with DRM technology.
- Developing techniques for secure multimedia broadcasting in wireless systems.

- Developing security and copyright techniques for home entertainment, such as IP-TV and digital TV, etc.
- Developing techniques for real-time multimedia processing for encryption and/or watermarking.
- Design of side channel attack resistant embedded systems to enable secure DRM systems.
- Developing low-power DRM technology for portable appliances.

This special issue presents research results in some of these areas. However, existing research has to make much progress before effective real-time DRM systems can be developed. We hope researchers, educators, students, and industry, who are interested in such systems will greatly benefit from this special issue.

2. Scanning the Special Issue

Deepthi, John, and Sathidevi proposed a new model for Linear Feedback Shift Register (LFSR) based keystream generation. They combine two schemes, such as the nonlinear combination generators and clock-controlled generators in the model. Field-Programmable-Gate-Array (FPGA) implementations of the two schemes are presented for a comparative perspective.

Ghavami, Pedram, and Najibi proposed an automatic synthesis flow for design of side channel attack resistance encryption chips. The synthesis flow considers a high-level description of a system and generates hardware using a special standard cell library. Proof of concept for Data Encryption Standard (DES) and Advanced Encryption Standard (AES) algorithms showed 23% power reduction compared to existing data driven asynchronous synthesis method.

Guha, Bagherzadeh, and Chou proposed a Memory-Aware Run-Time Reconfigurable Embedded System or MARTRES for efficient resource management and performance improvement of video streaming applications. They evaluated their approach for H.264/MPEG4 video compression algorithms which are widely used for storing and transmitting enormous amount of video data, in DVD, HDTV and wireless phones.

Zhang, Yang, and Gao presented a privacy-aware secure processor design for hardware assisted streaming media protection (H-SMP) against key sharing. The authors compare different protection policies and highlighted hardware enhancements, such as instruction set extensions for supporting protection policies.

Deepthi, Nithin, and Sathidevi presented three different versions of Pseudorandom Bit Generators (PRBG) based on Elliptic Curves over prime. The authors prototyped the algorithms on FPGA and compared their time complexities and sequences in terms of periodicity. They first identified Pseudo Random Bit Generators (PRBG) most suitable for software and hardware implementation. Then, they provided a comparative implementation in software and VHDL.

Gelbart, Leontie, Narahari, and Simha proposed a system called CODESSEAL for protection of software in embedded system based on a joint compiler-hardware approach. The approach utilizes a compiler based software tool, and an on-chip FPGA-hardware that provides run-time integrity checking.

Ghosh, Alam, Chowdhury, and Gupta presented two parallelization techniques and architectures to speed up the GF(p) elliptic curve multiplication in affine domain. The proposed

architectures were demonstrated to provide better thoughput than existing approaches, and to be resistant to side-channel-attacks.

Kougianos, Mohanty, and Mahapatra presented an exhaustive survey of the hardware assisted solutions proposed in the literature for watermarking of multimedia objects. The survey is preceded by an introduction to the background issues involved in digital watermarking. Then different FPGA-based, custom-IC based, and DSP board based hardware solutions for watermarking are presented. They are compared in terms of technology, power consumption, and performance. Both image and video watermarking chips are discussed. The survey ends with discussion on challenges and future directions.

Moradi, Taghi, Shalmani, and Salmasizadeh introduced a logic style for side channel attack resistant cryptographic hardware design. The technique is based on transition signaling that utilizes two wires for each signal and a bit value is transmitted by a transition on a selected wire. The authors proposed to use T-flip-flops to build dual-rail-transition logic (DTL) parts. DTL randomizes power dissipations and makes the circuit side channel attack proof.

Wang and Huang introduced a software key container in on-line media services that can provide security to user's key. The authors combine a human-trapdoor distortion function and symmetric cipher for protection of the key. The authors claim that it is computationally infeasible to break the system by using only a machine attack. The primary idea is that users must participate and verify each password that is guessed in the attack.

Jamkhedkar and Heileman presented an open layers framework in which different technologies can interact towards the development of Digital Rights Management (DRM) systems. The authors studied interoperability in the context of the framework. The authors also presented architecture to implement a DRM environment. It is learned that refactoring of current rights expression languages (RELs) based on a set of design principles is necessary to achieve a reasonable level of DRM interoperability.

Wang, Liu, and Masilela proposed a scalable MPEG2 watermarking scheme using a parallel architecture for real-time performance. The authors proposed a content-based block selection algorithm to efficiently embed the pseudo-random watermarks into DCT blocks. The authors claim that the proposed system can support real-time watermarking for high-resolution (up to 1404 x 960) video by solving the memory-shortage bottleneck.

Maity, Kundu, and Maity introduced Fast Walsh Transform (FWT) based spread-spectrum image watermarking approach for the dual purposes of authentication in data transmission as well as QoS assessment for digital media. The authors claim that FWT offers low computation cost for implementation, smaller change in image information due to data embedding, and ease of hardware realization. The authors also present an FPGA based implementation to satisfy real-time requirements.

Acknowledgements

We gratefully acknowledge the reviewers (listed in Appendix I) who contributed their invaluable expertise and time toward this special issue. We received a total of 29 submissions out of which 13 were selected for this issue based on their feedback. We thank all the authors who submitted their original research results to this special issue for consideration. We thank the

editorial staff of the journal for publishing the papers. We thank Prof. Paris Kitsos, Hellenic Open University, Patras, Greece, for inviting us to serve as editors for this issue. Our special thanks also go to Editor-in-Chief, Prof. Mo Jamshidi for bringing this issue.

References

[1] Emmanuel, S., Kankanhalli, M.S.: A Digital Rights Management Scheme for Broadcast Video. ACM-Springer Verlag Multimedia Systems Journal, 8 (2003) 444–458.
[2] Kundur, D., Karthik, K.: Digital Fingerprinting and Encryption Principles for Digital Rights Management. Proceedings of the IEEE, 52 (2004).
[3] Mohanty, S. P., Ranganathan, N., and Namballa, S. P.: A VLSI Architecture for Visible Watermarking in a Secure Still Digital Camera (S^2DC) Design, IEEE Trans. Very Large Scale Integration Systems, 13 (7) 2005, 808-818.
[4] Mathai, N. J., Kundur, D., and Sheikholeslami, A.: Hardware Implementation Perspectives of Digital Video Watermarking Algortithms, IEEE Trans. on Signal Processing, 51 (4), 925–938, April 2003.
[5] Alfonsi, B.: I want my IPTV: Internet Protocol television predicted a winner, IEEE Distributed Systems Online, Feb. 2005.
[6] Cherry, S.: The battle for broadband [Internet protocol television], IEEE Spectrum, Feb. 2005.
[7] http://www.digitalwatermarkingalliance.org/, accessed on April 2008.
[8] http://www.digimarc.com/, accessed on April 2008.

Saraju P. Mohanty is currently an Assistant Professor at the Dept. of Computer Science and Engineering, University of North Texas (UNT) is the founding director of the VLSI Design and CAD Laboratory (VDCL). He obtained his Ph.D. from University of South Florida, ranked among the top 50 public Universities in the USA with leadership in low-power VLSI research, in Fall 2003. He obtained his masters in System Science and Automation from the highest ranked institute from India, the Indian Institute of Science, Bangalore, in 1999. His bachelor's degree in Electrical Engineering is from the College of Engineering and Technology, Orissa University of Agriculture and Technology, Bhubaneswar, that ranks among top 50 engineering institutes in India. His research is in "Design and CAD for Low-Power High-Performance Nanoscale VLSI". He develops power, leakage, and performance models, incorporates them in CAD flow through optimization methodology, and demonstrates them through computational intensive multimedia applications. His research is currently funded by National Science Foundation (NSF). Dr. Mohanty is an author of 70 peer-reviewed top-notch journal and conference publications, many of which have been nominated for best paper awards. They have received worldwide citations, a total of approximately 150, till date. He is an author of a book titled "*Low-Power High-Level Synthesis for Nanoscale CMOS Circuits*", due release in June 2008. He serves on the program committee of several international conferences. He is a member of ACM, IEEE, ACM-Special Interest Group in Design Automation, IEEE-Circuits and Systems Society, IEEE-Computer Society, and IEEE-Consumer Electronics Society.

Nasir Memon is a Professor in the Computer Science Department at Polytechnic University, New York. He is the director of the Information Systems and Internet Security (ISIS) lab at Polytechnic (http://isis.poly.edu). His research interests include Data Compression, Computer and Network Security, Digital Forensics, and Multimedia Data Security.

Karam S. Chatha received the B.E. (with honors) degree in computer technology from Bombay University, Kalina, Mumbai, in 1993, and M.S and and Ph.D. degree in computer science and engineering from University of Cincinnati in 1997 and 2001, respectively. He is currently an Assistant Professor in the Department of Computer Science and Engineering at the Arizona State University. His research interests are centered on topics related to application specific digital system design, including architectures, design methodologies, and computer-aided design (CAD) tools. In particular, he has focused on Network-on-Chip (NoC) design, multiprocessor System-on-Chip (MPSoC) programming, hardware-software co-design, and reconfigurable and adaptive computing. Dr. Chatha is a recipient of the NSF CAREER Award 2006, and best paper awards at International Conference of Computer-Aided Design (ICCAD) 2007, and International Workshop on Field Programmable Logic (FPL) 1999. He is a member of the ACM

Appendix I

List of Reviewers with Affiliations

Alapan Arnab, University of Cape Town, South Africa
Ali Akoglu, University of Arizona, USA.
Andreas Uhl, Salzburg University, Austria
Aviral Shrivastava, Arizona State University, USA.
Bhagirath Narahari, George Washington University, USA
Cuneyt Taskaran, Motorola, USA
Debargah Mukherjee, HP labs, USA
Dhruva Ghai, University of North Texas, USA
Dijiang Huang, Arizona State University, USA.
Elaheh Bozorgzadeh, University of California, Irvine, USA
Elias Kougianos, University of North Texas, USA
Emir Dirik, Polytechnic University, USA
Hae Yong Kim, University of Sao Palo, Brazil
Hefei Ling, Huazhong University of Science and Technology, China
Ismail Avcibas, Uludag University, Turkey
Jimson Mathew, University of Bristol, UK.
Jonathan Liu, University of Florida, USA
Joseph Zambreno, Iowa State University, USA
Limin Liu, Purdue University, USA
Lin Zhong, Rice University, USA.
Manuel Hilty, Swiss Federal Institute of Technology, Switzerland
Mehrdad Nourani, University of Texas, Dallas, USA
Ming Jiang, Polytechnic University, USA
Naehyuck Chang, Seoul National University, Korea
Nelly Fazio, IBM Almaden, USA
Nicholas Sheppard, University of Wollogong, Australia
Partha Dasgupta, Arizona State University, USA.
Peetabasa Pati, Indian Institute of Science, Bangalore, India
Pranab Mohanty, University of South Florida, USA
Praveen S. Bhojwani, Texas A & M University, USA
Regu Radhakrishnan, Dolby Labs, USA
Roman Lysecky, University of Arizona, USA
S. J. Ruan, National Taiwan University of Science & Technology, Taiwan
Sabu Emmanuel, National University of Singapore, Singapore
Samuel Leshner, Arizona State University, USA
Sarojananda Mishra, Indira Gandhi Institute of Technology, India
Siddartha Tambat, Indian Institute of Science, Bangalore, India
Sunita Nayak, University of South Florida, USA
Takaaki Yamada, Hitachi, Japan
Victor Faye-Wolfe, University of Rhode Island, USA
Wy Yongdong, Institute for Infocomm Research, Singapore