2010 Joint Workshop between Tohoku University and National Tsing Hua University

15-16 December, 2010

Akiu Resort Hotel Sakan (Yumoto Akiu, Taihaku-Ku, Sendai 982-0241, Japan)

Scientific Program:

15 December, 2010

10:30-10:40 Opening [Meeting Room Shippo]

Michitaka Kameyama (Dean of Graduate School of Infrmation Sciences, Tohoku University)

Keh-Yung Cheng (Dean of College of Electrical Engineering and Computer Science, National Tsing Hua University)

10:40-11:30 Prenary Session [Meeting Room Shippo]

Kazuo Hashimoto (GSIS, Tohoku University)
Title: Personalized health-care service and its service infrastructure

11:30-13:30 Lunch

13:30-15:30 VLSI Session [Meeting Room Shippo]

Ting-Ting Hwang (Dept. CS, National Tsing Hua University)
Title: Run-time reconfiguration of expandable cache for embedded systems

Masanori Hariyama (GSIS, Tohoku University)
Title: Accelerator-centric design methodologies for heterogeneous multi-core processors

Chih-Tsun Huang (Dept. CS, National Tsing Hua University)
Title: High-throughput VLSI design for dual-field elliptic curve cryptography

Masanori Natsui (RIEC, Tohoku University)
Title: High-yield VLSI design using emerging functional devices and its impact

13:30-15:30 Multi-Media and Machine Learning Session [Meeting Room Horai]

Candy Hsu (Dept. CS, National Tsing Hua University)
Title: Age estimation using facial feature projection with personalized ranking constraints

Kazuyuki Tanaka (GSIS, Tohoku University)
Title: Bayesian image analysis by belief propagation

Chia-Wen Lin (Dept. EE, National Tsing Hua University)
Title: Digital erasers: Video inpainting for dynamic textured background and occluded objects

Yuji Waizumi (GSIS, Tohoku University)
Title: Applications in statistical pattern recognition and machine learning

Hwann-Tzong Chen (Dept. CS, National Tsing Hua University)
Title: Object localization using feature distributions

15:30-15:45 Break

15:45-17:00 Student Poster Session [Meeting Room Horai]
Spotlight Presentations (15:45-16:00) [Meeting Room Horai]
Poster Presentations (16:00-17:00) [Meeting Room Horai]

18:30-20:30 Banquet

16 December, 2010

9:30-10:30 Student Poster Session
Poster Presentations (9:30-10:30) [Meeting Room Horai]

List of Speakers in Student Poster Sessions

1. **An-Chi Chang** (Dept. CS, National Tsing Hua University)
   Title: Synthesis of multi-bit flip-flops for clock power reduction
2. **Jyu-Yuan Lai** (Dept. CS, National Tsing Hua University)
   Title: Design framework for high-performance elliptic curve cryptographic processors
3. **Zhengfan Xia** (GSIS, Tohoku University)
   Title: Self-timed wave-pipelined circuits using synchronizing logic gates
4. **Nobuaki Okada** (GSIS, Tohoku University)
   Title: Fine-grain multiple-valued reconfigurable VLSI based on logic-in-control architecture
5. **Yi-Lei Chen** (Dept. CS, National Tsing Hua University)
   Title: Time-variant modeling for general surface appearance
6. **Tetsuharu Sakurai** (GSIS, Tohoku University)
   Title: Approximate learning algorithm for restricted Boltzmann machines
7. **Tsuyoshi Sato** (GSIS, Tohoku University)
   Title: Network application identification using sequential transition patterns of payload length

Co-sponsered by

Department of Computer Science, National Tsing Hua University, Taiwan
Graduate School of Information Sciences (GSIS), Tohoku University, Japan
Global COE (Center of Excellence) Program "Center of Education and Research for Information Electronics Systems"

Abstracts of
2010 Joint Workshop between Tohoku University and National Tsing Hua University

15-16 December, 2010

Akiu Resort Hotel Sakan (Yumoto Akiu, Taihaku-Ku, Sendai 982-0241, Japan)

Prenary Session

Personalized health-care service and its service infrastructure

Kazuo Hashimoto, Graduate School of Information Sciences, Tohoku University, Japan

Japan, along with many developed countries, is facing severe social problems such as increased needs for various social services such as elderly care while the working population is gradually shrinking. Next generation ubiquitous services must be developed to address these problems, considering individual personal circumstances and at socially acceptable cost. These ubiquitous social services will evolve toward enhanced pervasiveness, and will be defined as advanced personalized services.

VLSI Session

Run-time reconfiguration of expandable cache for embedded systems

Ting-Ting Hwang, Department of Computer Science, National Tsing Hua University, Taiwan

Expandable cache proposed by G. Bournoutian and Orailoglu is very efficient in reducing miss rate and energy consumption with small area overhead. However, in the original expandable cache, using only MSB for cache expansion may lead to thrashing problems. In this work, based on the structure of expandable cache, we will introduce a new cache design which has more flexible expansion schemes to fit different run-time program behaviors. The expansion scheme of our proposed cache design is dynamically changed by executing configuration instructions which are inserted at compile time.

Accelerator-centric design methodologies for heterogeneous multi-core processor

Masanori Hariyama and Michitaka Kameyama, Graduate School of Information Sciences, Tohoku University, Japan

Heterogeneous multi-core processors are attracted by the media processing applications due to their capability of drawing strengths of different cores to improve the overall performance. However, the data transfer bottlenecks between different cores becomes a serious problem. This paper presents two key methodologies to solve the data transfer bottolenecks: memory allocation considering a addressing function constraint and task allocation based on algorithm transformation.

High-throughput VLSI design for dual-field elliptic curve cryptography

Chih-Tsun Huang, Department of Computer Science, National Tsing Hua University, Taiwan

As the demand of electrical communication keeps exploding, data security has become an urgent need for modern vital applications. Among various data security schemes, Elliptic Curve Cryptography (ECC) is robust and effective for the secure data transaction and messaging. We will introduce our design of a high-throughput, parallel, and scalable elliptic curve cryptographic processor. A two-phase scheduling methodology is proposed to optimize the ECC arithmetic over both finite fields. Our dual-field ECC architecture supports arbitrary elliptic curves and arbitrary finite fields with different field sizes. The optimization to a variety of applications

with different area/throughput requirements can be achieved rapidly and efficiently. The comparison of speed and area overhead among different ECC designs justifies the cost-effectiveness of the proposed ECC architecture with its design methodology

High-yield VLSI design using emerging functional devices and its impact

Masanori Natsui, Takahiro Hanyu, Research Institute of Electrical Communication, Tohoku University, Japan

We have been developing novel multi-functional device-based VLSI design methodology as a so-called "More Than Moore" approach for VLSI processors with both high-performance and highly dependable capabilities. In this presentation, we demonstrate the principle of an yield-enhancement technique based on a new VLSI design paradigm called "nonvolatile logic-in-memory architecture", and its possibility for the design of high-yield VLSI through the analysis of a process-variation-aware logic-in-memory circuit component.

Multi-Media and Machine Learning Session

Age estimation using facial feature projection with personalized ranking constraints

Candy Hsu, Department of Computer Science, National Tsing Hua University, Taiwan

The appearance of human faces changes with age significantly. It is still a big challenge to estimate age from the appearance of facial images. In this talk, we focus on the application of age estimation from facial images. We try to improve the accuracy of age estimation from two aspects. First, we propose to analyze facial features by projecting into nonnegative bases, which could better interpret the nonnegative image representation than mixed-sign bases. Our simulations also show that using nonnegative bases could effectively characterize local facial appearance change. Second, we propose to select mid-level features on the manifold space with personalized ranking constraints. We conduct experiments on the publicly available FG-NET database and compare the estimation results with existing methods. The experimental results show that the proposed ranking manifold would efficiently preserve the structure of aging tendency.

Bayesian image analysis by belief propagation

Kazuyuki Tanaka, Graduate School of Information Sciences, Tohoku University, Japan

Bayesian network is one of the methods for probabilistic inferences in artificial intelligence. Some probabilistic models for image processing are also regarded as Bayesian networks. In this talk, the statistical aspect and the practical schemes of Bayesian network to probabilistic image processing are reviewed. The first part is an introduction of probabilistic model for image processing based on the basic framework of Bayesian networks. The second part is a brief review of belief propagation. In the third part, we survey fundamental algorithms of belief propagations for probabilistic image processing. Some recent developments of Bayesian networks and belief propagations in computer sciences are also shown. Bayesian network is one of the methods for probabilistic inferences in artificial intelligence. Some probabilistic models for image processing are also regarded as Bayesian networks. In this talk, the statistical aspect and the practical schemes of Bayesian network to probabilistic image processing are reviewed. The first part is an introduction of probabilistic model for image processing based on the basic framework of Bayesian networks. The second part is a brief review of belief propagation. In the third part, we survey fundamental algorithms of belief propagations for probabilistic image processing. Some recent developments of Bayesian networks and belief propagations in computer

sciences are also shown.

Digital erasers: Video inpainting for dynamic textured background and occluded objects

Chia-Wen Lin, Department of Electrical Engineering National Tsing Hua University, Taiwan

This talk will summarize our research work in developing digital eraser tools for intelligent video editing. When removing an unwanted object from a video using an editing tool, there will an object hole that need to be filled in with static textured background, dynamic textured background, or an occluded object. How to maintain spatio-temporal coherence in an inpainted video is a critical problem. Mosaics-based copy-and-paste approaches may do a good job in static textured background inpainting; however, it is not suitable for inpainting a scene with time-varying texture (a.k.a. dynamic texture). To address the problem, we propose applying manifold learning to dynamic texture synthesis to obtain an incomplete low-dimensional trajectory of dynamic textured background with holes. As for occluded object inpainting, we propose two approaches: one is based on virtual contour-guided posture retrieval and the other is based on manifold learning-based posture sequence estimation. Experimental results show that the proposed methods achieve promising subjective qualities.

Applications in statistical pattern recognition and machine learning

Yuji Waizumi, Graduate School of Information Sciences, Tohoku University, Japan

In this presentation, two applications in statistical pattern recognition and machine learning are introduced. One application is handwritten character recognition with our original model of Neural Networks. This is one model of Multi Layered Perceptron (MLP) and has “squared connection” which can make the model represent gauss-like distribution. Another application introduced in this presentation is “Network Application Identification”. Although port number which is recorded in a network packet is commonly used to identify the type of application of traffic of computer networks, the identification with port numbers is not reliable because it can be tampered easily. To tackle this problem, a statistical pattern recognition approach is applied to network application identification. By extracting features of each network application from its traffic, statistical pattern recognition technique can identify the type of application of observed traffic.

Object localization using feature distributions

Hwann-Tzong Chen, Department of Computer Science, National Tsing Hua University, Taiwan

We present two approaches to finding objects in images. Both approaches use feature distributions as the appearance model for objects. In the first approach, we introduce an efficient pixel-sampling technique to find the location of the target in a large image, by comparing the feature histogram of the target with the feature histograms of candidate subwindows in the test image. We adopt the probability-product kernels as the similarity measures, and show that the computation of feature histograms and the evaluation of the kernel-based similarities can be integrated through a time-and memory-efficient sampling process. In the second approach, we address the problem of finding the common salient objects that appear in both of a given pair of images. The proposed algorithm simultaneously handles feature selection and object localization according to the feature distributions of objects. Under the setting of co-saliency detection, our algorithm uses the joint information provided by the image pair to inhibit the feature responses of objects that appear in just one of the two images, and thus is able to identify the common salient objects inside image pairs.

Student Poster Session

Synthesis of multi-bit flip-flops for clock power reduction

An-Chi Chang, Department of Computer Science, National Tsing Hua University, Taiwan

Multi-bit flip-flop has shown to be effective in power and area reduction through sharing of clock signal. We proposed a novel power optimization method by iteratively merging flip-flips to share common signals, while considering placement density and timing slack constraints. Experimental results based on industry benchmark show that our approach can effectively reduce power consumption and area.

Design framework for high-performance elliptic curve cryptographic processors

Jyu-Yuan Lai, Department of Computer Science, National Tsing Hua University, Taiwan

Our design framework for Elliptic curve Cryptographic (ECC) processors will be presented for the cost-effectiveness design exploration. Our parallel and scalable ECC architecture supports for arbitrary elliptic curves and finite fields. With the proposed scheduling optimization approaches, different levels of parallelism among design hierarchies can be explored systematically. Based on our methodology, several test chips have also been designed and fabricated to justify the effectiveness.

Self-timed wave-pipelined circuits using synchronizing logic gates

Zhengfan Xia, Shota Ishihara, Masanori Hariyama and Michitaka Kameyama, Graduate School of Information Sciences, Tohoku University, Japan

This paper introduces a novel self-timed pipeline design which greatly reduces the handshake-circuit overhead and offers high throughput as well as low power consumption. The pipeline has a latch-free operation/handshake-control integrated structure which is suitable for fine-grain pipelining. The pipeline is composed of Synchronizing Logic Gates (SLGs) and Synchronizing Logic Gates with Latch function (SLGLs). An SLG is a dual-rail dynamic gate which can synchronize the input signal and has a small gate-delay variation. Based on SLGs, SLGLs are extended which can be used as latches to block signal transfer. Using the characteristics of SLGs and SLGLs, the slowest datapath becomes predicable. With the information of the slowest datapath, the pipeline structure is optimized, which greatly reduces the overhead of handshake circuits.

Fine-grain multiple-valued reconfigurable VLSI based on logic-in-control architecture

Nobuaki Okada and Michitaka Kameyama, Graduate School of Information Sciences, Tohoku University, Japan

A fine-grain digit-serial multiple-valued reconfigurable VLSI is proposed for effective use of the hardware resources. Resource sharing allocation where one or more nodes in a control/data flow graph are mapped into a single arithmetic/logic circuit makes it possible to reduce the number of the arithmetic/logic circuits. In the resource sharing allocation, control and the arithmetic/logic circuits are constructed by using one or multiple cells, where a cell consists of a logic block and switch block. In the logic-in-control architecture, only one state in a state transition diagram is allocated to one cell to implement the control circuit, which leads to reduction of the complexity of interconnections between cells. A 3-variable binary operation is required for implementing the control circuit, and the hardware resource is shared as a common hardware resource for the arithmetic/logic circuit to make the high utilization ratio of the cell. The fine-grain cell is implemented based on multiple-valued current-mode circuit technology. Multiple-valued signal transfer between cells and a linear

summation just by wiring are effectively employed for reduction of the area of the cell.

Time-variant modeling for general surface appearance

Yi-Lei Chen, Department of Computer Science, National Tsing Hua University, Taiwan

Describing time-variant appearance of object surface is still an open problem. With intricate environmental factors and different material characteristics over time, no researcher did tackle the principal problem: how to formulate time-variant change on general surface appearance? In this presentation, we attempt to solve this challenging issue. Using multi-linear algebra representation, we propose a novel appearance model and characterize the surface-specific and time-variant properties. When given an unknown sample, we propose a robust method to estimate its aging degree. In addition, we also propose an approach to synthesize its realistic appearance changes even when the material of this given sample does not exist in our database. Experimental results demonstrate the feasibility and effectiveness of our proposed approach. To the best of our knowledge, this challenging issue is first explored in image processing applications.

Approximate learning algorithm for restricted Boltzmann machines

Tetsuharu Sakurai, Muneki Yasuda, and Kazuyuki Tanaka, Graduate School of Information Sciences, Tohoku University, Japan

Deep Belief Networks (DBNs) are Bayesian networks with many layers of hidden units which were recently introduced along with a greedy layer-wise learning algorithm by Hinton et al. In the learning algorithm, the main building block of a DBN is a bipartite undirected graphical model called Restricted Boltzmann machine (RBM). Hinton et al. used approximate learning algorithms called contrastive divergences to learn RBMs, but in 2008 Roux and Bengio proposed new learning algorithm for RBMs, which is more suitable for the greedy layer-wise learning procedure of DBNs. However, Roux and Bengio's learning algorithm includes costly calculation whose amount is proportional to the square of the number of training data. In this presentation, we propose a new fast learning algorithm for RBMs by applying an approximate method called Kullback-Leibler Importance Estimation Procedure to Roux and Bengio's learning algorithm. We also show its validity by comparing our proposed algorithm with Roux and Bengio's learning algorithm using numerical experiments based on artificial data.

Network application identification using sequential pattern of payload lengths

Tsuyoshi Sato, Yuji Waizumi and Kazuyuki Tanaka, Graduate School of Information Sciences, Tohoku University, Japan

Recently, an increasing of information leakage incidents caused by the illegal use of network applications has been reported. To prevent such incidents, a network administrator should check and block the traffic exchanged by unauthorized applications, such as P2P file sharing software. Therefore, a method is needed to quickly identify network applications without port numbers, because port numbers can be easily spoofed. In this presentation, a method to identify applications using sequential pattern of payload lengths of packets is introduced. Trough experiments using real network traffic, the identification performance of our method is demonstrated.