External Awards

Best Paper Award

Winner: Kazumaro Aoki[†1], Takeshi Shimoyama[†1], Toshikazu Homma[†2], and Hiroki Ueda[†1]
†1 NTT Information Sharing Platform Laboratories
†2 Fujitsu Laboratories Ltd.
Date: October 30, 2007
Organization: ISEC of ESS in IEICE and CSEC in IPSJ

For "Experiments on the Linear Algebra Step in the Number Field Sieve".

This paper shows experimental results of the linear algebra step in the number field sieve on a parallel environment with implementation techniques. We developed an efficient algorithm that shares the sum of vectors in each node, and the network structure among the nodes only needs to include a ring. We also investigated the construction of a network for the linear algebra step. The construction can be realized through switches and network interface cards, which are not expensive. Moreover, we investigated the implementation of the linear algebra step using various parameters. The implementation described in this paper was used for the integer factoring of a 176 digit number by GNFS and a 274 digit number by SNFS.

ECC Technology Award

Winner: Tatsuaki Okamoto, NTT Information Sharing Laboratories
Date: November 13, 2007
Organization: Certicom ECC Conference 2007

For "ECC and the MOV Attack".

The MOV attack on a specific class of ECC was discovered around 17 years ago (in 1990) by Alfred Menezes, Scott Vanstone, and myself, when I was visiting Prof. Vanstone at the University of Waterloo. This was just 5 years after the idea of ECC was independently proposed by Koblitz and Mille.

International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM 2007) Best Paper Award

Winner: Kazumasa Takami[†1], Toshikazu Homma[†1], and Shinichiro Goto[†2]
†1 Faculty of Engineering, Soka University
†2 NTT Information Sharing Platform Laboratories
Date: December 11, 2007
Organization: International Academy, Research, and Industry Association (IARIA)

For "A Method of Deducing a User's State of Mind from an Analysis of the Pictographic Characters Used in Mobile Phone Emails".

As the ubiquitous environment is taking root, services that deliver content appropriate for the individual user's personal interests and preferences are required. However, it is difficult to deduce the ever-changing preferences of people. This paper proposes a method of deducing the state of mind of the user by analyzing the pictographic characters in his or her mobile phone emails.

Papers Published in Technical Journals and Conferences

Automatic Composition of Color Ocular Fundus Images

K. Tanabe, T. Tsubouchi, H. Okuda, and M. Oku
IEICE Trans. on Information and Systems (Japanese ed.), Vol. J90-D, No. 9, pp. 2595–2605, 2007.

This paper describes a PC-based system that is able to automatically combine color ocular fundus images captured from different angles by a digital retinal camera. The system matches the locations of retinal vascular nodes (crossing points or branches) in the different images by comparing the correlation values of all nodes in a particular rectangular area with all other nodes in all other rectangular areas. In an experiment involving 28 volunteers, the system successfully generated, in real time, composite ocular fundus montages from the 9 color ocular fundus images taken of each volunteer. It was able to match 246 out of 252 images and automatically generated 23 montages without operator intervention. This system is therefore very promising for the automatic assembly of color ocular fundus montages.

"Save YourSelf !!!": An Experience of Transplanting the Sense of Balance

H. Ando, T. Yoshida, T. Maeda, and J. Watanabe
TVRSJ, Vol. 12, No. 3, pp. 225–232, 2007.

We have developed a novel sensation interface using galvanic vestibular stimulation (GVS). The vestibular system is stimulated by weak current through the electrodes, placed behind the ears. GVS causes lateral virtual acceleration toward the anode, which shifts the sense of balance. The GVS interface can induce lateral walking diverging from an intended straight line. Based on this GVS interface technology, we produced an artwork on the subject of wavering identity in the modern society. In our artwork, the compact display is floating on water. An acceleration sensor is integrated into the display, and the obtained data is sent to the GVS interface. GVS is presented according to the data from the sensor. Any kind of vibration of the display disturbs the balance of the wearers. When the display falls over, they feel a big swaying sensation. This GVS interaction makes them feel truly connected to the display. They keep on walking, while holding the tank of water. This artwork is intended to observe and hold your wavering identity (the display on the water) from the outer

perspective.

Double-layer Slider-Crank Mechanism to Generate Pulling or Pushing Sensation without an External Ground

T. Amemiya, I. Kawabuchi, H. Ando, and T. Maeda

Proc. of the 2007 IEEE/RSJ IROS, Oct. 29–Nov. 2, San Diego, CA, USA.

When a small object in a hand-held device moves periodically and prismatically with asymmetric acceleration (strong in one direction and weak in the other), the holder typically experiences the kinesthetic illusion of being pushed or pulled continuously by the held device. We investigated this perceptual effect for its potential application to a hand-held, non-grounded, haptic device that can convey a sense of a continuous translational force in one direction, which is a yet missing tile in haptics research. A one-degree-of-freedom haptic device based on a two-symmetric-slider-crank mechanism was constructed to convert the single-speed rotational cyclic movement of a motor into asymmetric translational cyclic movement with asymmetric acceleration and to cancel unwanted side acceleration. We verified our previous results with the haptic device and investigated the effect of the gross weight of the device on force perception.

A Multichannel Linear Prediction Method for the MPEG-4 ALS Compliant Encoder

Y. Kamamoto, N. Harada, and T. Moriya

WASPAA 2007, IEEE, Oct. 21–24, NY, USA.

A new linear prediction analysis method for multichannel signals was devised, with the goal of enhancing the compression performance of the MPEG-4 Audio Lossless coding (ALS) compliant encoder. The multichannel coding tool for this standard carries out an adaptively weighted subtraction of the residual signals of the coding channel from those of the reference channel, both of which are produced by independent linear prediction. Our linear prediction method tries to directly minimize the amplitude of the predicted residual signal after subtraction of the signals of the coding channel. The results of a comprehensive evaluation show that this method yields a 0.1% smaller compressed file size on average, the maximum improvement of compression ratio achieves 14.6%, at the cost of a small increase in computational complexity at the encoder and without increase in decoding time. This is a practical method because the compressed bit stream remains compliant with the MPEG-4 ALS standard.

Certificate-less User Authentication with Consent

S. Orihara,Y. Tsuruoka, and K. Takahashi

Workshop on Digital Identity Management (DIM 2007), ACM, Vol. 1, No. 1 pp. 11–16, Fairfax, USA, 2007.

We introduce a new authentication scheme that is intended to be used on electronic commerce (EC) sites, which do not require strict user authentication but need user identification. That is, the EC sites judge whether a user is the same person who visited the site before. We designed our scheme to be as simple and lightweight as possible, for example, we do not assume the existence of trusted third parties (TTPs), e.g., CAs, which are not necessarily needed to identify users. We noticed that password-based authentication has a property that enables EC sites to confirm that there was an interaction with the user. This can be used to show that the user confirmed some agreement. This confirmation of agreement is sometimes important for EC sites. Our scheme can change how to combine password-based authentication and public-key-based authentication by its authentication policy, such as required security level and necessity of confirmation of agreement.

Analysis of Interior Degradation of a Laser Waveguide Using an OBIC Monitor

T. Takeshita, R. Iga, M. Yamamoto, and M. Sugo

We propose a novel optical-beam-induced current (OBIC) measurement technique for detecting the degradation in the interior of a waveguide. This technique uses an incident light with a wavelength longer than that of the band edge of the active layer. An OBIC scan image was obtained at a wavelength of 1.6 μm, which was 50 nm longer than the PL peak wavelength in the active layer of the degraded laser, and the OBIC became sensitive to some degradation when a long distance guided light was used. Furthermore, we confirmed that the degradation mechanism of the $t^{0.5}$ deterioration property is mainly governed by diffused defects at the waveguide other than those in the vicinity of the AR facet in a DFB laser.