Foundation of Computer Science Laboratory

Takafumi Hayashi
Professor

Shuxue Ding
Professor

Yodai Watanabe
Assistant Professor

Zhang Hongiuan
Visiting Researcher

The research and education activities in the laboratory focus on the theoretical foundations of computers and computations, including broad applications in computer science and engineering. Our work covers algorithms and computation, programming languages, discrete mathematics, statistical signal processing, cryptography, neuro-computing, optimization, simulated acoustics and related topics.

Areas of our research interest include

- Combinatorics and its applications;
- Application of Information Geometry to Big Data analysis
- Application of Robust Computational Geometry and Ultra Discrete to Information Geometry
- Spread spectrum communication;
- Sparse representation and sparse component analysis;
- Content-Aware networking;
- Secure Cloud Computing, SOA, xAAS;
- Quantum cryptography,
- Signal processing;
- Image analysis for measurement;
- Enterprise Integration and Messaging Network:

- Information Security Management;
- Networks;
- GRID as a Service Oriented Architecture Based System;
- Security and management of computer system for e-Government;
- Blind source separation and independent component analysis, and their applications in acoustic signals and vital signs;
- Neural computing and brain-style signal processing;
- Optimization and machine learning;
- Time-reversal wave propagation in ergodic environment and its applications in acoustics, ultrasonics and telecommunications;
- Information theory and algorithmic complexity.
- smart grid
- radar pulse compression

The following combined research is running:

- independent component analysis and sequence design.
- independent component analysis and network anomaly detection.
- distributed data store grids loosely coupled integration and cryptography.

Faculty of the FCS laboratory teach Computer Literacy, Programming I, Algorithms and Data Structures, Advanced Algorithms, Digital Signal Processing, Statistical Signal Processing, Introduction to Topology, Information Security, SCCPs and other selective courses. Students join faculty research and also develop their own research themes. We participate in various research projects of JSPS, NIFS, RIKEN etc.

Refereed Journal Papers

[takafumi-01:2012] Takafumi Hayashi, Takao Maeda, and Shinya Matsufuji.

Refereed Proceeding Papers

[sding-04:2012] Hongjuan Zhang, Zikai Wu, Shuxue Ding, and Luonan Chen. A fixed-point blind source extraction algorithm and its application to ECG data analysis. In Luonan Chen, Xiang-Sun Zhang, Ling-Yun Wu, and Editors Yong Wang, editors, *Proc. IEEE 6th International Conference on Systems Biology*, pages 73–78. IEEE ISB, IEEE, August 2012.

Generalized autocorrelations and complexity pursuit are two recently developed methods for extracting interesting component from time series. They are the extensions of projection pursuit to time series data. In this paper, a fixedpoint blind source extraction (BSE) algorithm for generalized autocorrelations and complexity pursuit of the desired signals is presented. The fixed-point algorithm inherits the advantages of the well-known FastICA algorithm of ICA, which is very simple, converges fast, and does not need to choose any learning step sizes. Numerical experiments on electrocardiogram (ECG) data indicate its better performance.

[takafumi-03:2012] Takafumi Hayashi, Shigeru Kanemoto, and Takafo Maeda. Sequence sets having wide inter-subset zero-correlation zone and its applications to instrumentation. In *Proc. SICE 2012*, pages 1150–1155. SICE, Sept. 2012.

The present paper introduces the construction of a class of sequence sets with zero-correlation zones called zero-correlation zone sequence sets. The proposed zero-correlation zone sequence set can be constructed if there exist positive integers (N_d) and a non-negative integer $m \geq 0$, $S = \pm 1$ that satisfy the criterion $L_p = (Z+1)N_d = (TL_b - S + \Lambda)N_d$ for the length L_p of the given perfect sequence *pseq* and there exists a Hadamard matrix of order $(Z+1)m + L_b$. The proposed sequence set has *vnum* subsets. The correlation function of the sequences of a pair of different subsets referred to as the *inter-subset correlation function*, has a zero-correlation zone with a width that is approximately $(\Lambda + 1)$ times that of the correlation function of the sequences of the same subset (*intra-subset correlation function*). This wider inter-subset

zero-correlation enables the improvement in performance of applications of the proposed sequence set. The proposed scheme can improve radars using the zero-correlation property of the sequence set.

[takafumi-04:2012] Takao Maeda and Takafumi Hayashi. Fourier Analysis of Sequences over a Composition Algebra of the Real Number Field. In *Proc. ISITA 2012*, pages 34–39. ISITA, Sept. 2012.

To analyze the structure of a set of perfect sequences over a composition algebra of the real number field, transforms of a set of sequences similar to DFT (discrete Fourier transform) are introduced. Discrete cosine transform, discrete sine transform and generalized discrete Fourier transform (GDFT) of the sequences are defined and the fundamental properties of these transforms are proved. We show that GDFT is bijective and that there exists a relationship between these transforms and a convolution of sequences. Applying these properties to the set of perfect sequences, a parameterization theorem of such sequences is obtained.

[takafumi-05:2012] Takafumi Hayashi, Hideyuki Fukuhara, Yodai Watanabe, Junya Terazono, Taro Suzuki, Masayuki Hisada, Tetsu Saburi, and Atsushi Kara Jiro Iwase. A Network-Centric Approach to Low-Power Consumption Sensor-network with Related Service Integration. In *Proc. SICE 2012*, pages 1433–1336. SICE, Sept. 2012.

The present paper describes an approach to reduce the power consumption of a sensor network using a content-aware network so called messaging network. A messaging network can be constructed as a structured overlay network. The proposed scheme enables loosely-coupled integration of sensor data and related services. Message mediation enables inter-operation of various applications and integration of diverse sensor data. The policy mediation, which is a kind of message mediation, for over-lay networks having each own policies enables secure overlay networks inter-operation. The proposed approach can realize and maintain a total power consumption optimization of an intelligent infrastructure, which can provide various kinds of functions including data processing, and computing. The proposed data store grids helps to construct and manage as secure, flexible, elastic, and sustainable loosely coupled integration of sensor data and related services.

[yodai-01:2012] Kotaro Yoshida and Yodai Watanabe. Security of audio secret sharing scheme encrypting audio secrets. In *Proceedings of the 7th*

International Conference for Internet Technology and Secured Transactions (ICITST-2012), pages 294–295. IEEE, December 2012.

Secret sharing is a method of encrypting a secret into multiple pieces called shares so that only qualified sets of shares can be employed to reconstruct the secret. Audio secret sharing (ASS) is an example of secret sharing whose decryption can be performed by human ears. This paper proposes the first ASS schemes encrypting audio secrets whose security is rigorously evaluated in terms of the mutual information between secret and shares.

Unrefereed Papers

[takafumi-06:2012] 村澤政成, 戸倉一, 山崎治郎, 阿部泰裕, 福原英之, 宮崎敏明, 矢口勇一, 岡隆一, 岩瀬次郎, and 林隆史. ネットワークセントリックに関連する情報の動的関連づけのための情報基盤. In **情報処理学会全国大会** *2013* **講演論文集**, volume 2013, pages 369–371. 情報処理学会, 2013.

network centric 手法を用いて real-time 情報を結合統合したシステムの設計・構築方法と、実証実験結果を報告した。

[takafumi-07:2012] 寺薗淳也, 山崎治郎, 久田雅之, 戸倉一, 鈴木太郎, 渡辺曜大, 矢口勇一, 成瀬継太郎, 宮崎敏明, 福原 英之, 岩瀬次郎, and 林 隆史. グラフデータベースを用いたサービス疎結合支援基盤. In *2012* **年社会情報学会** *(SSI)* **研究発表大会**, 2012.

セキュアなクラウドの利活用では、柔軟かつ安全なサービスの疎結合が大きな意味を持つ。サービス、アプリケーションからネットワークの下位層まで含めて、多様な選択肢のなかから、その時々で最善の組み合わせによる連携をすばやく実現することが、重要である。我々はネットワークセントリックな手法でサービスの疎結合を支援する情報基盤を提案してきた。今回、グラフデータベースを用いることで、より柔軟な情報基盤を提案した。。

[takafumi-08:2012] 山崎治郎, 陳　健, 吉野大志, 高橋友一, 丹野嘉信, 阿部泰裕, 戸倉一, 福原英之, 佐分利徹, 藤田龍太郎, and 林隆史. メッセージングネットワークのスマートグリッドへの応用に向けて. In **信学技報** *IA2012-72*, volume 112, pages 7–11, 2012.

As one of the next generation electric power systems, the Smart Grid is expected that can integrate a variety of information organically, and contribute to energy saving and environmental protection. In this study, the information such as the electricity consumption, weather, electric rate and bill, electricity supply and demand, storage battery and location involves wide fields, which is considered to be used for the smart grid. The standards of how to save

or which format is used to save the information may be formulated by international standards from now, but some of them perhaps have not been standardized yet. In addition, it ' s necessary to find a way that can bridge the differences between the similar or the same standards used in the different fields. In order to solve these problems, we propose an approach of combining the applications or information for the smart grid by using the messaging network.

[takafumi-09:2012] 福原 英之, 佐分利 徹, 藤田 龍太郎, 宮崎 敏明, 渡辺曜大, 岩瀬次郎, 加羅淳, 林 隆史, and 久田雅之. サステナブルな 100 年データストアの構築・運用. In *2012* 年国際 *C I O* 学会秋季研究大会, 2012.

message network を使って、長期にわたって、運用可能なデータストアを可能にする方法を提案した。

[takafumi-10:2012] 宮崎敏明, 林　隆史, 束原恒夫, Song Guo, and 北道淳司. 零相関系列セットを用いた超音波イメージング. In 信学技報 *US2010-20*, volume 112, pages 63–68. IEICE, 2012.

We propose a wide-area sensing system that can mash up the sensed data with useful information obtained from other existing systems, and display them on the user terminal. To get appropriate sensed data quickly and effectively, the system seeks the sensed data based on the ambiguous sensing demand given by the user, and customizes the sensor network dynamically if necessary. The sensor network itself has environment adaptability that the role of each sensor node can be changed autonomously in consideration of the environmental situation and the user demand so as to collect the required sensed data. In this paper, an overview of the proposed technologies is introduced using an application of monitoring wide-area disaster-hit regions as an example.

[takafumi-11:2012] 伊藤悠哉, 戸倉一, 山崎治郎, 阿部泰裕, 福原英之, 宮崎敏明, 岩瀬次郎, and 林隆史. 大規模かつ多様なデータをリアルタイム解析のための情報基盤. In *IPSJ* 全国大会講演論文集, volume 2013, pages 373–375. 一般社団法人情報処理学会, 2013.

network centric 手法を用いた real-time リアルタイム解析システムの設計・構築方法と、実証実験結果を報告した。

Grants

[takafumi-12:2012] Toshiaki Miyazaki, Tsuneo Tsukahara, Takafumi Hayashi, Song Guo, and Junji. Demand Addressable Sensor Network : A-STEP, 2012.

In this research project, novel demand addressable sensor network is researched

[takafumi-13:2012] Juni Yatabe, Takafumi Hayashi, and Yodai Watanabe. Health Care Information Infrastructure for high-blood pressure Patients : JSTP, 2012.

In this research project, Health Care Information Infrastructure for high-blood pressure is researched

[takafumi-14:2012] Jiro Iwase, Takafumi Hayashi, Yodai Watanabe, Taro Suzuki, and Toshiaki Miyazaki. IT 融合による新産業創出のための研究開発事業（産学官 IT 融合コンソーシアム拠点の整備）, 2012.

In this research project, an intelligent infrastructure for new business creation is researched

[takafumi-15:2012] Jiro Iwase, Takafumi Hayashi, Jiro Yamazaki, Hajime Tokura, and Incheon Paik. 地域イノベーション戦略支援プログラム（東日本大震災復興支援型）, 2012.

In this research project, an intelligent infrastructure for Regional Innovation is researched

[takafumi-16:2012] Takafumi Hayashi, Toshiaki Miyazaki, Takao Maeda, Tsuneo Tsukahara, and Yodai Watanabe. Novel Sequence Desig for Instrumentation :科研費 (基盤 C), 2012.

In this research project, various kinds of novel sequence are designed in order to develop a new insturmentaion for physics research and improve the performance of various kinds of instrumentation and communications.

[yodai-02:2012] Yodai Watanabe. Fukushima Prefectural Foundation for Advancement of Science and Education, 2012.

Academic Activities

[sding-05:2012] S. Ding, 2012.

Review committee member for Grants-In-Aid for Scientific Research Projects, JSPS; Performed the first stage reviewing.

[sding-06:2012] S. Ding, 2012.

Committee member of Technical Committee on Awareness Computing, Systems, Man & Cybernetics Society, IEEE.

[sding-07:2012] S. Ding, 2012.

Program Committee member of the 10th International Conference on Latent Variable Analysis and Signal Separation (LVA ICA 2012).

[sding-08:2012] S. Ding, 2012.

Program Committee member of The Seventh International Conference on Innovative Computing, Information and Control (ICICIC2012) and Fifth International Symposium on Intelligent Informatics (ISII2012).

[sding-09:2012] S. Ding, 2012.

Organizing & Program Committee member of the First Mini Symposium on Intelligent Informatics (MSII2012).

[sding-10:2012] S. Ding, 2012.

Institute of Electrical and Electronics Engineers (IEEE), Membership.

[sding-11:2012] S. Ding, 2012.

IEEE Signal Processing Society, Membership.

[sding-12:2012] S. Ding, 2012.

IEICE, Membership.

[sding-13:2012] S. Ding, 2012.

The Association for Computing Machinery (ACM), Membership.

[takafumi-17:2012] Takafumi Hayashi, 2012.

Reviewer of IEEE Signal Processing Letters

[takafumi-18:2012] Takafumi Hayashi, 2012.

Reviewer of ICC, IEEE

[takafumi-19:2012] Takafumi Hayashi, 2012.

Reviewer of IEEE Communication Letters

[takafumi-20:2012] Takafumi Hayashi, 2012.

Reviewer of IEICE Transactions

[takafumi-21:2012] Takafumi Hayashi, 2012.

Reviewer of OE Magazine, SPIE

[takafumi-22:2012] Takafumi Hayashi, 2012.

Reviewer of Eletctronics Letters, IET

[takafumi-23:2012] Takafumi Hayashi, 2012.

Program Chair of CIT2012

Ph.D and Others Theses

[sding-14:2012] Zunyi Tang. PhD. Thesis: Dictionary Learning Algorithms for Sparse Representation of Signals, University of Aizu, 2012.

Thesis Advisor: Shuxue Ding

[sding-15:2012] Ryutaro Kobayashi. Graduation Thesis: Independent Component Analysis Using Artificial Bee Colony Algorithm, University of Aizu, 2012.

Thesis Advisor: Shuxue Ding

[sding-16:2012] Yoshitaka Ozaki. Graduation Thesis: Independent Component Analysis by Batch Processing with the P-Norm as the Cost Function, University of Aizu, 2012.

Thesis Advisor: Shuxue Ding

[sding-17:2012] Sei Sano. Graduation Thesis: Independent Component Analysis without Whitening Using by Generalized Random-Tunneling Algorithm, University of Aizu, 2012.

Thesis Advisor: Shuxue Ding

[takafumi-24:2012] Koichi Sato. Graduation thesis, School of Computer Science and Engineering, 2013.

Thesis Advisor: T. Hayashi

[takafumi-25:2012] Keisuke Furukawa. Graduation thesis, University of Aizu, 2013.

Thesis Advisor: T. Hayashi

[takafumi-26:2012] Yuya Ito. Graduation thesis, School of Computer Science and Engineering, March 2013.

Thesis Advisor: T. Hayashi

[takafumi-27:2012] Nattachot Dusitanon. Master thesis, Graduate School of Computer Science and Engineering, August 2012.

Thesis Advisor: T. Hayashi

[takafumi-28:2012] Koji Hashima. Master thesis, Graduate School of Computer Science and Engineering, March 2013.

Thesis Advisor: T. Hayashi

[takafumi-29:2012] Masanari Murasawa. Graduation thesis, School of Computer Science and Engineering, 2013.

Thesis Advisor: T. Hayashi

[takafumi-30:2012] Kazuki Yatsui. Graduation thesis, School of Computer Science and Engineering, 2013.

Thesis Advisor: T. Hayashi

[takafumi-31:2012] Takahiro Shimazaki. Graduation thesis, School of Computer Science and Engineering, March 2012.

Thesis Advisor: T. Hayashi

[takafumi-32:2012] Ymenosuke Kokata. Graduation thesis, School of Computer Science and Engineering, 2013.

Thesis Advisor: T. Hayashi

[yodai-03:2012] Haruka Otaka. Graduation Thesis: Efficient Visual Secret Sharing Scheme Encrypting Multiple Images, University of Aizu, 2012.

Thesis Advisor: Y. Watanabe

[yodai-04:2012] Masaki Ando. Graduation Thesis: Integer Factorization by the Elliptic Curve Method, University of Aizu, 2012.

Thesis Advisor: Y. Watanabe

[yodai-05:2012] Hiroki Seino. Graduation Thesis: Implementation of the AKS primality test, University of Aizu, 2012.

Thesis Advisor: Y. Watanabe

[yodai-06:2012] Keiko Terunuma. Graduation Thesis: Spam filter utilizing normalized compression distance, University of Aizu, 2012.

Thesis Advisor: Y. Watanabe

[yodai-07:2012] Youta Matsuzaki. Graduation Thesis: Complex Network of the Board Game Go, University of Aizu, 2012.

Thesis Advisor: Y. Watanabe

Others

[yodai-08:2012] Yodai Watanabe, December 2012.

Session Chair, ICITST-2012