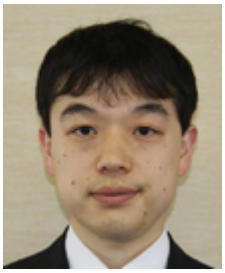
Foundation of Computer Science Laboratory

Takafumi Hayashi
Professor

Shuxue Ding
Professor



Yodai Watanabe
Associate Professor

Yen Neil Yuwen
Associate Professor

TSAI Joseph Cheng-wei
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;
- Modern cryptography including quantum cryptography;
- Introduction to Human-centeric Computing;
- Introduction to Big Data Science;
- 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
- Computational Geometry
- Information Theory

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, Linear Algebra II, Calculus I Quantum Information, SCCPs and other selective courses. Students join faculty research and also develop their own research themes. Our labolatory participate in various research projects of JSPS, NIFS, RIKEN, ISM, AIST, University of Tokyo, Kyoto Univesity, and Tohoku University.

Refereed Journal Papers

[neilyyen-01:2014] Frederick Li Benjamin Wah Rynson W.H. Lau, Neil Y. Yen. Recent development in multimedia e-learning technologies. *World Wide Web Journal*, 17(2):189–198, 2014.

[neilyyen-02:2014] Tun-Wen Pai Min-Ho Chang Hui-Huang Hsu, Neil Y. Yen. Personal Health Management on a Smartphone Platform. *Biomedical Engineering: Applications, Basis and Communications*, 26(4):1440004, 2014.

[neilyyen-03:2014] James J. Park Huang-Hua Tseng-Neil Y. Yen Chia-Chen Chen, Tien-Chi Huang. A Smart Assistant for Product-Awareness Shopping. *Personal and Ubiquitous Computing*, 18(2):339–349, 2014.

[neilyyen-04:2014] Kuo-Chung Chu Neil Y. Yen Lun-Ping Hung, James J. Park. Content-oriented Learning Recommendation Mechanism in MANETs. *International Journal of Ad Hoc and Ubiquitous Computing*, 15(4):252–262, 2014.

[neilyyen-05:2014] Neil Y. Yen Timothy K. Shih Hui-Huang Hsu Martin M., Wen-Chih Chang. Detection of Misconceptions and Misleading Questions by Using Quantitative Diagnostic Assessment. *International Journal of Distance Education Technology*, 12(2):26–50, 2014.

[sding-01:2014] H. Zhang, G. Wang, P. Cai, Z. Wu, and S. Ding. A Fast Blind Source Separation Algorithm Based on the Temporal Structure of Signals. *Neurocomputing (Elsevier)*, 139(9):261–271, 2014.

Classical independent component analysis (ICA) has been reasonably successful; however, the performance and the convergence of the conventional ICA algorithms have reached limitations of further improvement since they utilize only the statistical independency among the sources. For circumventing this situation, in this paper, we incorporate some other kinds of temporal priori information, i.e., the generalized autocorrelation and the nonlinear predictability of each source, and make a convex combination of them to formulate a novel cost function for blind source separation (BSS). With this cost function, a fixed-point BSS algorithm is developed. This algorithm inherits the advantages of the well-known FastICA algorithm of ICA, which converges fast and does not need to choose any learning step sizes. Its higher separation accuracy is verified by numerical experiments. Meanwhile, we

also give the consistency analysis and prove convergence properties of the algorithm, which has a (locally) consistent estimator and at least quadratic convergence.

[takafumi-01:2014] Takafumi Hayashi, Takao Maeda, Shigeru Kanemoto, and Shiya Matsufuj. Low-Peak-Factor Pseudo-White-Noise Sequence Set with Optimal Zero-Correlation Zone. *IEICE Trans. Fundamentals*, E97-A(12):2343–2351, Dec. 2014.

The present paper introduces a novel method for the construction of sequences that have a zero-correlation zone. For the proposed sequence set, both the cross-correlation function and the side lobe of the autocorrelation function are zero for phase shifts with in the zero-correlation zone. The proposed scheme can generate a set of sequences, each of length $16n^2$, from an arbitrary Hadamard matrix of order n and a set of $4n$ trigonometric function sequences of length $2n$. The proposed construction can generate an optimal sequence set that satisfies, for a given zero-correlation zone and sequence period, the theoretical bound on the number of members. The peak factor of the proposed sequence set is equal to $\sqrt{2}$.

Refereed Proceeding Papers

[neilyyen-06:2014] Jianhua Ma Neil Y. Yen, Runhe Huang. Social network based smart grids analysis. In *IEEE International Symposium on Independent Computing (ISIC)*, pages 1–6, 2014.

Renewable energy is an important research issue in recent years, it's also regarded by most of the governments in the world. In order to manage or employ the power well, the aspect of smart gird is proposed to process many kinds of situations renewable energy. Power scheduling is one of the focal points in this research field. By this work, users can understand the volume of power consumption and decide a finer province electricity plan. Based on this concept, renewable energy generation prediction is the approach to enhance the power scheduling and performance of power using. We propose a prediction approach by the theory of social networking and machine learning. We use the SVM, its kernel is RBF, to process the power generation prediction by weather forecasts. The social networking is used to improve the accuracy of the prediction. In the experimental result, the accuracy rate is showed with the excellent results.

[sding-02:2014] Y. Li, S. Ding, and Z. Li. A Dictionary-Learning Algorithm for the Analysis Sparse Model with a Determinant-Type of Sparsity Measure. In *Proc. the 19th International Conference on Digital Signal Processing*, pages 152–156, Hong Kong, China, August 2014. DSP 2014, IEEE.

Dictionary learning for sparse representation of signals has been successfully applied in signal processing. Most the existing methods are based on the synthesis model, in which the dictionary is overcomplete. This paper addresses the dictionary learning and sparse representation with the so-called analysis model. In this new model, the analysis dictionary multiplying the signal can lead to a sparse outcome. Though it has been studied in the literature, there is still not an investigation in the context of nonnegative signal representation, which should not be a trivial problem. In this paper, moreover, we propose to learn an analysis dictionary from signals using a determinant-type of sparsity measure. In the formulation, we adopt the Euclidean distance as the error measure. Based on these, we present a new algorithm for the dictionary learning and sparse representation. Numerical experiments on recovery of analysis dictionary show the effectiveness of the proposed method.

[sding-03:2014] Z. Li, S. Ding, Y. Li, Z. Tang, and W. Chen. Improving dictionary learning using the Itakura-Saito divergence. In *Proc. 2014 IEEE China Summit & International Conference on Signal and Information Processing*, pages 733–737, Xi'an, China, July 2014. IEEE Signal Processing Society, IEEE.

This paper presents an improved and efficient algorithm for overcomplete, nonnegative dictionary learning for nonnegative sparse representation (NNSR) of signals. We adopt the Itakura-Saito (IS) divergence as the error measure, which is quite different from the conventional dictionary learning methods using the Euclidean (EUC) distance as the error measure. In addition, for enforcing the sparseness of coefficient matrix, we impose l1-norm minimization as the sparsity constraint. Numerical experiments on recovery of a dictionary show that the proposed dictionary learning algorithm performs better than other currently available algorithms which use Euclidean distance as the error measure.

[takafumi-02:2014] Joseph C. Tsai, Neil Y. Yen, and Takafumi Hayashi. Social Network based Smart Grids Analysis. In *Proc. IEEE SSCI 2014*, pages 1–6. IEEE, Sept. 2014.

Renewable energy is an important research issue in recent years, it ' s also regarded by most of the governments in the world. In order to manage or employ the power well, the aspect of smart gird is proposed to process many kinds of situations renewable energy. Power scheduling is one of the focal points in this research field. By this work, users can understand the volume of power consumption and decide a finer province electricity plan. Based on this concept, renewable energy generation prediction is the approach to enhance the power scheduling and performance of power using. We propose a rediction approach by the theory of social networking and machine learning. We use the SVM, its kernel is RBF, to process the power generation prediction by weather forecasts. The social networking is used to improve the accuracy of the prediction. In the experimental result, the accuracy rate is showed with the excellent results.

[takafumi-03:2014] Takafumi Hayashi, Junichi Yatabe, Sayaka Demura, Yasuhiro Abe, Yodai Watanabe, Hiroaki Ishikawa, Masayuki Hisada, Midori S. Yatabe, Daishi Yoshino, Joseph Tsai, Yuya Ito, Hayato Tabata, Masanari Murasawa, Kyohei Shiozawa, Toshiaki Miyazaki, , and Jiro Iwase. A Novel Network-centric Approach to a Secure and Elastic Regional Healthcare System with a Messaging Infrastructure. In *Proc. SICE 2014*, pages 252–258. SICE, Sept. 2014.

This paper introduces an intelligent infrastructure scheme for regional health care systems that uses a messaging network to provide message filtering, routing, and related services via a structured overlay network. The proposed messaging network, which will provide various functions using content/topic-based routing and filtering, also provides the backbone of our proposed regional healthcare system. Additionally, the design of a regional hypertensive patient management system (RHPMS) that uses the proposed scheme is presented, and a sample implementation of an RHPMS under construction in the Aizu region of Fukushima Prefecture in Japan is described. When complete, the design and performance of the system will be evaluated via substantive experiments with an eye towards improvements.

[takafumi-04:2014] Takafumi Hayashi, Yodai Watanabe, and Takao Maeda. A Novel Class of Binary Zero-Correlation Zone Sequence Sets by using a Cyclic Difference Set. In *Proc. ISITA 2014*, pages 663–667. IEICE, Oct. 2014.

The present paper introduces the construction of a binary sequence that has a zero-correlation zone (ZCZ). For the proposed sequence set, the cross-

correlation function and the side-lobe of the autocorrelation function are zero for the phase shifts within the zero-correlation zone. The proposed ZCZ sequence set can be generated from an arbitrary binary sequence that has a two-value autocorrelation. In actual applications, the peak of the correlation function for the phase outside of the zero-correlation zone is important. The absolute value of the out-of-phase correlation function of the proposed sequence of length m-th is less than or equal to $2^{m+1}(n+1)$, which is about half of the power (the inner product) $2^{m+2}n$ of the sequence. The proposed sequence set can be used in a robust sensor/controller network. With the proposed sequence, we examine the performances of ultrasonic imaging and the ambiguity function of radar pulse compression.

[takafumi-05:2014] Jiro Yamazaki, Joseph Tsai, Daishi Yoshino, Hideyuki Fukuhara, Hajime Tokura, and Takafumi Hayashi and Jiro Iwase. A Network-Centric Approach to Sensor-Network for Smart Grid. In *Proc. ICRERA 2014*, pages 241–244. ICRERA, Oct. 2014.

This paper provides an approach for data processing infrastructure in next generation of smart grid, which would be more complicated with heterogeneous factors, such as renewable energy resources, electric vehicles, microgrids, smart meter, demand-side energy management system, demand response, and dynamic-pricing. To solve this complicated environment, key technology is information technologies and then this paper proposes a scheme and data processing framework with analytic infrastructure for future Smart Grid, which would make innovative application and service with effective development.

[takafumi-06:2014] Takafumi Hayashi, Yodai Watanabe, and Takao Maeda. A Novel Zero-Correlation Zone Sequence Set Having a Low-Peak Factor and a Flat Power Spectrum. In *Proc. ISITA 2014*, pages 668–672. IEICE, Oct. 2014.

The present paper introduces a novel method for the construction of sequences that have a zero-correlation zone. For the proposed sequence set, both the cross-correlation function and the side lobe of the auto-correlation function are zero for phase shifts within the zero-correlation zone. The proposed sequence set can be generated from an arbitrary Hadamard matrix of order n and a set of $2n$ trigonometric-like function sequences of length $4n$. The proposed construction can generate an optimal sequence set that satisfies the theoretical bound on the number of members for the given zero-correlation zone and sequence period. The auto-correlation function of the

proposed sequence is equal to zero except for the phase shift 0. The peak factor of the proposed sequence set is $\sqrt{2}$.

[takafumi-07:2014] Takao Maeda and Takafumi Hayashi. Parameterization of high-dimensional perfect sequences over a composition algebra over R. In *Proc. ISITA 2014*, pages 682–686. IEICE, Oct. 2014.

To analyze the structure of a set of high-dimensional perfect sequences over a composition algebra over R, we developed the theory of Fourier transforms of such sequences. Transforms that are similar to discrete Fourier transforms (DFTs) are introduced for a set of sequences. We define the discrete cosine transform, the discrete sine transform, and the generalized discrete Fourier transform (GDFT) of the sequences, and we prove the fundamental properties of these transforms. We show that the GDFT is bijective and that there exists a relationship between these transforms and a convolution of sequences. By applying these properties to a set of perfect sequences, we obtain a parameterization theorem for the sequences. Using this theorem, we show the equivalence of the left and right perfectness.

[yodai-01:2014] Manami Sasaki and Yodai Watanabe. Formulation of visual secret sharing schemes encrypting multiple images. In *39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014)*, pages 7391–7395, Florence, Italy, May 2014. IEEE.

Secret sharing is a method of generating multiple shares from secret information so that only a qualified set of shares can be employed to recover this secret information. Visual secret sharing (VSS) is an example of secret sharing; its decryption can be performed by using human eyes without a computer. This paper provides a formulation of encryption for multiple secret images, which is a generalization of the existing ones, and also a general method of constructing VSS schemes encrypting multiple secret images.

[yodai-02:2014] Shinya Washio and Yodai Watanabe. Security of audio secret sharing scheme encrypting audio secrets with bounded shares. In *39th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2014)*, pages 7396–7400, Florence, Italy, May 2014. IEEE.

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 examines the security of an audio secret sharing scheme encrypting audio secrets with bounded shares, and optimizes the security with respect to the probability distribution used in its encryption.

[yodai-03:2014] Takafumi Hayashi, Yodai Watanabe, and Takao Maeda. A Novel Class of Binary Zero-Correlation Zone Sequence Sets by Using a Cyclic Difference Set. In *International Symposium on Information Theory and Its Applications (ISITA 2014)*, pages 650–654, Melbourne, Australia, October 2014. IEICE.

The present paper introduces the construction of a binary sequence that has a zero-correlation zone (ZCZ). For the proposed sequence set, the cross-correlation function and the side-lobe of the autocorrelation function are zero for the phase shifts within the zero-correlation zone. The proposed ZCZ sequence set can be generated from an arbitrary binary sequence that has a two-value autocorrelation. In actual applications, the peak of the correlation function for the phase outside of the zero-correlation zone is important. The absolute value of the out-of-phase correlation function of the proposed sequence of length m is less than or equal to $2^{m+1}(n+1)$, which is about half of the power (the inner product) $2^{m+2}n$ of the sequence. The proposed sequence set can be used in a robust sensor/controller network. With the proposed sequence, we examine the performances of ultrasonic imaging.

[yodai-04:2014] Takafumi Hayashi, Yodai Watanabe, Shinya Matsufuji, and Takao Maeda. A Novel Zero-Correlation Zone Sequence Set Having a Low-Peak Factor and a Flat Power Spectrum. In *International Symposium on Information Theory and Its Applications (ISITA 2014)*, pages 655–659, Melbourne, Australia, October 2014. IEICE.

The present paper introduces a novel method for the construction of sequences that have a zero-correlation zone. For the proposed sequence set, both the cross-correlation function and the side lobe of the auto-correlation function are zero for phase shifts within the zero-correlation zone. The proposed sequence set can be generated from an arbitrary Hadamard matrix of order n and a set of $2n$ trigonometric-like function sequences of length $4n$. The proposed construction can generate an optimal sequence set that satisfies, for a given zero-correlation zone and sequence period, the theoretical bound on the number of members. The peak factor of the proposed sequence set is equal to $\sqrt{2}$.

Unrefereed Papers

[takafumi-08:2014] Takafumi Hayashi, Takao Maeda, Shinya Matsufuji, and Yodai Watanabe. Synchronization and Positioning using Binary Zero-Correlation Zone Array. In *Proc. of Annual Conf. of JSIAM*, volume 2014, pages –. JSIAM, 2014.

A novel scheme of Visible Secret Sharing using Binary Zero-Correlation Zone Array is proposed. The proposed scheme enables the position matching of images for visible secrete sharing.

Grants

[sding-04:2014] Shuxue Ding. Research on the source signal recovery and shape image reconstruction from data with incomplete information based on sparse representation, 2011-2014.

This is supported as the project of Scientific Research C, No. 24500280, 2011 Grants-In-Aid for Scientific Research, Ministry of Education, Culture, Sports, Science and Technology, Japan.

[takafumi-09:2014] Takafumi Hayashi, Toshiaki Miyazaki, Takao Maeda, Tsuneo Tsukahara, and Yodai Watanabe. Novel Sequence Desig for Instrumentation :Grant-in-Aid for Scientific Research (C) (Kakenhi), 2012-2014.

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.

[takafumi-10:2014] Toshiaki Miyazaki, Tsuneo Tsukahara, Takafumi Hayashi, Song Guo, and Junji. Demand Addressable Sensor Network : A-STEP, 2012-2014.

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

[takafumi-11:2014] Junichi Yatabe, Takafumi Hayashi, and Yodai Watanabe. Health Care Information Infrastructure for high-blood pressure Patients : JSTP, 2012-2014.

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

[takafumi-12:2014] Jiro Iwase, Takafumi Hayashi, Jiro Yamazaki, Hajime Tokura, and Incheon Paik. Fukushima Regional Innovation Project, 2012-2016.

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

Academic Activities

[sding-05:2014] S. Ding, 2014.

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

[sding-06:2014] S. Ding, 2014.

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

[sding-07:2014] S. Ding, 2014.

IEEE Signal Processing Society, Membership.

[sding-08:2014] S. Ding, 2014.

The Institute of Electronics, Information and Communication Engineers (IEICE), Membership.

[sding-09:2014] S. Ding, 2014.

The Association for Computing Machinery (ACM), Membership.

[takafumi-13:2014] Takafumi Hayashi, 2014.

Reviewer of IEICE Transactions

[takafumi-14:2014] Takafumi Hayashi, 2014.

Reviewer of OE Magazine, SPIE

[takafumi-15:2014] Takafumi Hayashi, 2014.

Reviewer of Eletctronics Letters, IET

[takafumi-16:2014] Takafumi Hayashi, 2014.

Program Chair of SICET2014

[takafumi-17:2014] Takafumi Hayashi, 2014.

Reviewer of IEEE Signal Processing Letters

[takafumi-18:2014] Takafumi Hayashi, 2014.

Reviewer of IEEE Communication Letters

[takafumi-19:2014] Takafumi Hayashi, 2014.

Reviewer of ICC, IEEE

Patents

[yodai-05:2014] Yodai Watanabe. Visual secret sharing method and program, 2014.

Ph.D and Others Theses

[sding-10:2014] Kengo Sato. Graduation Thesis: Independent Component Analysis for Sub-Gaussian Distributed Signals, University of Aizu, 2014.

Thesis Advisor: Shuxue Ding

[sding-11:2014] Shiori Watanabe. Graduation Thesis: Effcient Nonnegative Matrix Factorization for Sparse Coding Based on the Auxiliary Function Method, University of Aizu, 2014.

Thesis Advisor: Shuxue Ding

[sding-12:2014] Yoshitaka Ozaki. Master Thesis: Online Independent Component Analysis for Separation of Signals including Super-Gaussian and Sub-Gaussian Components, University of Aizu, 2014.

Thesis Advisor: Shuxue Ding

[takafumi-20:2014] Akihiro Onomura. Graduation thesis, School of Computer Science and Engineering, 2014.

Thesis Advisor: T. Hayashi

[takafumi-21:2014] Yoshihiko Kondo. Graduation thesis, School of Computer Science and Engineering, 2014.

Thesis Advisor: T. Hayashi

[takafumi-22:2014] Kenta Monma. Graduation thesis, University of Aizu, 2014.

Thesis Advisor: T. Hayashi

[takafumi-23:2014] Shodai Watanabe. Graduation thesis, School of Computer Science and Engineering, March 2014.

Thesis Advisor: T. Hayashi

[takafumi-24:2014] Atsunori Tezuka. Graduation thesis, School of Computer Science and Engineering, March 2014.

Thesis Advisor: T. Hayashi

[takafumi-25:2014] Hayato Tabata. Master thesis, Graduate School of Computer Science and Engineering, March 2014.

Thesis Advisor: T. Hayashi

[takafumi-26:2014] Kyohei Shiozawa. Master thesis, Graduate School of Computer Science and Engineering, March 2014.

Thesis Advisor: T. Hayashi

[takafumi-27:2014] Yuya Ito. Master thesis, Graduate School of Computer Science and Engineering, March 2014.

Thesis Advisor: T. Hayashi

[takafumi-28:2014] Masanari Murasawa. Master thesis, Graduate School of Computer Science and Engineering, March 2014.

Thesis Advisor: T. Hayashi

[takafumi-29:2014] Koichi Saito. Master thesis, Graduate School of Computer Science and Engineering, March 2014.

Thesis Advisor: T. Hayashi

[yodai-06:2014] Kazuya Hashimoto. Graduation Thesis: Complex Networks of the Board Game Shogi, University of Aizu, 2015.

Thesis Advisor: Y. Watanabe

[yodai-07:2014] Yuki Onuma. Graduation Thesis: Security Evaluation of Audio Secret Sharing Scheme, University of Aizu, 2015.

Thesis Advisor: Y. Watanabe

[yodai-08:2014] Kiyohito Miura. Graduation Thesis: Complex Networks of the '01 Game of Darts, University of Aizu, 2015.

Thesis Advisor: Y. Watanabe

Others

[yodai-09:2014] Shinya Washio and Yodai Watanabe. Construction and Security of an Audio Secret Sharing Scheme with Bounded Shares (in Japanese), 2014.

2013 IPSJ Tohoku Section Young Scientist Award (Shinya Washio)