List of Dissertation Abstract （Information Media and Environment Sciences　Information Media Course）

Name	Supervisor	Title	Abstract
Yuya ABE	Katsunori OKAJIMA	Study on installation requirements about display on electronic in-car mirror and improvement of depth feel.	In recent years, electronic in-car mirrors are paid attention to by automobile industry. It has a lot of benefit in safety, but on the other hand it has some problems. This study aims to clarify visibility of display on electronic rear-view mirrors and to improve depth feel of display on electronic side-view mirrors by conducting experiments. As a result, the best installation condition and the formulation about display on electronic rear-view mirrors and the best curve condition to improve depth feel about display on electronic side-view mirrors were proposed.
Shunsuke Iida	Roger Martin	Aspectual Properties of Japanese Stative Verbs	The main purpose of the present study is to propose a new way of classifying Japanese verbs and especially to investigate the aspectual properties of Japanese Stative Verbs. We propesed some tests to clarify Japanese Stative Verbs preciously according to the differences of English *"V-ing"* and Japanese *-"V-teiru"-*. We have come to the conclusion that Japanese stative verbs can be classified into two groups: verbs expressing only states and verbs　expressing both states and processes leading up to the states.
Yuichi Ikeda	Tatsunori Mori	Study on Automated Methods to Extract Onomatopoeia Words from Japanese Text by Taking Accout of Derivation and Coined Words	We study automated methods to extract onomatopoeias from Japanese texts. First, we discuss a method to extract onomatopoeias of 3 moras or less, which is implemented as sequential labeling using phoneme information, classes of onomatopoeia patterns, and sequential labeling. Second, in order to extract derivatives of onomatopoeias, we take account of transformation rules of the derivation. Experimental results show the effectiveness of proposed methods.
Junichi IDA	Junji SHIKATA	Interactive Signcryption	In recent years,　an interactive encryption　and authentication have been proposed. The advantage of the interactive cryptography is possible to construct a scheme that meets strong security from weak cryptographic primitives as compared with non - interactive setting. However, signcryption which effectively achieve both the function of public-key encryption and digital signature simultaneously has been proposed yet. In this paper, we propose an interactive signcryption. First, we newly define a model and security notions of interactive signcryption. Second, we propose four generic constructions of interactive signcryption. Finally, we also give comparison our constructions from two points of view.

Tomohiro OMATA	Tatsunori MORI	Automatic Collection and Visualization of the Expressions that Represent Changes of Situations in the Society	In utilizing intellectual property, it is necessary to grasp the change in social situation. There are various ways in which we may find changes of situation in our society. For some of them, such as statistical information, we have to begin with discussion of how to interpret them. We, therefore, focus on expressions on Web documents that authors interpret as expressions of changes in situations of our society. We propose a method to collect them automatically from the Web documents. We also discuss visualization methods to help users to understand the collected expressions easily.
Taira OYAMA	Katsunari YOSHIOKA	Analysis of Malware and Decoy Document used for Targeted Email Attacks	Recently, targeted attacks which aim at a specific organization or individual have become great threats. However, the actual situation of targeted attacks is not fully understood, so we describe the study on grasping the actual situation of targeted attacks at intrusion stage and after invasion.
Daiki KAWANUMA	Tkashi TOMII	Implementation and Evaluation of Data Analysis Framework using ECOLOG Database	We have built a database to estimate electric vehicle energy consumption from driving logs. This study, examines a data analysis framework that aggregates numerous operation logs. Furthermore, we implement mobile application program for information presentation. Finally, we evaluated whether the function was satisfied.
Masaru KITAJIMA	Takashi TOMII	Construction of a Database capable of Investigation of Microgrid Introduction Effects using Lifelog and Showing of Information	In recent years, more and more microgrids are being installed. However, in order to examine the introduction effect of microgrid, it is necessary to use “logs about that place” and “logs at that time”. In this research, I designed an integrated database which accumulated life logs such as commuting logs by car and building electricity demand logs, and open data such as weather logs and social electricity demand logs. Also, I constructed a system which allows you to consider the introduction effect of microgrid which contained solar panels and EVs.
Hayato KOBAYASHI	Tatsunori MORI	Visualization of Web documents relationships based on discovery of network structure considering contents similarity	In recent years, with the advancement of computer performance and network development, electronic documents have been increasing, and there is a need for a technique that enables users to efficiently access necessary information from a large volume of documents.Documents obtained by information retrieval, which is one of them, are varied in point of view and degree of detail.Based on the above background, we propose organizing output for grasping contents efficiently by presenting a document covering various perspectives and a detailed document group on the viewpoint in the document in association with each other.

Shota GOTO	Junji SHIKATA	Cryptographic Protocols with Universally Composable and Game-Theoretic Security	In recent years, game-theoretic security of cryptographic protocols has been studied. Generally, cryptographic security is defined so as to guarantee some basic concrete properties when participants follow the designed algorithms, even if facing an adversarial behavior. In contrast, game-theoretic security is defined such that, by considering behaviors of rational participants in a protocol whose goal is to achieve their best satisfactions, following the specifications of the protocol honestly is the most reasonable for the rational participants. In this thesis, we consider the following question: Does composing protocols having game-theoretic security result in a secure protocol in the sense of game-theoretic security?
Midori SAITO	Tomoharu NAGAO	Image Enlargement based on Evolutionary Image Processing	In this paper, an evolutionary image processing based image enlargement is proposed. Evolutionary image processing is effective in various fields. In image enlargement process, a low-resolution image is down information, so we can consider some candidates of high-resolution images from one low-resolution image. The proposed approach enables to generate a number of possible images by an evolutionary image processing, and to control image complexity by fractal dimension. We studied optimization method and fitness function by the experiments generating enlarged images.
Junichi SAKAMOTO	Tsutomu MATSUMOTO	Security Studies: Implementation of Lightweight Block Cipher and Tamper Resistance for IoT End Devices	The study consists of two parts. IoT end devices have insufficient computational resources to perform cryptographic functions. The first study show that some lightweight block ciphers are available on such the resource-restricted devices. The second study propose that an attack that extracts memory data using a combination of laser and power analysis. Implementation attacks including the proposed method become practical attacks since IoT end devices are easily accessible by attackers. The study presents the importance of tamper resistance for IoT end devices.
Miho SAKITSU	Tomoharu NAGAO	4DCT images estimation from 3DCT images using Cartesian Genetic Programming	Radiation therapy is effective because it is a minimally invasive procedure. However, radiation exposure associated with acquisition of 4DCT images is more than that with acquisition of 3DCT; therefore, 4DCT imaging may be a concern for patients. In this thesis, we propose a method that estimates 4DCT images from 3DCT images using Cartesian Genetic Programming (CGP). During the training phase, features are extracted from 4DCT data, and the trajectories of the features in three-dimensional space are approximated using CGP. For estimation of 4DCT images from 3DCT images, trained CGP will be used to estimate trajectories of the extracted features.

Shingo SATO	Junji SHIKATA	Lattice-based Signcryption	Signcryption is a scheme achieving both functions of public-key encryptions and digital signatures, and important and fundamental protocol in cryptography. On the other hand, lattice-based cryptographies are based on the lattice problems and resistant to attacks using quantum computers. In this thesis, we propose lattice-based signcryption schemes. We show that our constructions are more efficient than existing ones by comparing these constructions in terms of key-size and ciphertext-size.
Ryo SANO	Tatsunori MORI	Recognition of Specific-General Relation among Condition Expressions for Interactive Generation of Condition-Conclusion Map	We study interactive generation of Condition – Conclusion Map, which is supposed to be used for supporting a user's judgement on the credibility of information on the Web.Given a statement on which a user focused, this system shows conclusions that are derived from the statement, and conditions in which the statements holds, in order for a user to be able to make a decision, whether to do the action represented by the statement, or not. In this thesis, we propose a method to identify general-specific relationship among statements to organize the statements in the Condition-Conclusion Map.
Satoshi SHIMIZU	Tomoharu NAGAO	Similar Drawing Retrieval Considering Relationship among Partial Regions	In similar drawings retrieval domain, Text-Based Image Retrieval using keywords previously given to drawings is generally performed. Although it is possible to narrow down candidates to a certain degree by the Text-Based Image Retrieval, the contents of drawings is very useful for further narrowing down. This thesis proposes a more efficient Content-Based Image Retrieval method to retrieve similar patent drawings considering relationship among partial regions using query images described by multiple figures. We consider relationship among partial regions of patent drawings and aim to achieve proposed method with high versatile.
Masato SHIRASAWA	Junji SHIKATA	A stufy on unconditionally secure homomorphic encryption	The fully homomorphic encryption is one of the cryptographies which gives processing function to specific encrypted data. We can operate ciphertexts without decrypting them. In this thesis, we propose a new security definition of perfect secrecy regarding fully homomorphic encryption based on unconditional security, and show the validity of this definition. We also propose a specific construction of fully homomorphic encryption scheme and show that this construction satisfies our definition.

Kento TOMATSU	Tomoharu NAGAO	Evolutionary Music Composition Considering Musical Forms of Songs	Automatic music composition has been researched for composing emotional and various songs. In this paper, we propose a music composition system considering musical forms of songs. In our method, songs which have musical forms of typical pops are composed by Genetic Algorithm. In order to compose songs considering forms, we introduce fitness functions that evaluate individuals not only from the viewpoint of music theory, but also from the viewpoint of part likeness and connection between parts. In addition, we aim to acquire the music that the user wants with less burden by adding modifications while incorporating the user's evaluation on the generated songs.
Risa NAKAGAWARA	Junji SHIKATA	On the Key Dependent Message Security of General Construction of Hybrid Encryption	Cryptosystems are technologies to do secure communication on information networks,and three FO conversions are proposed to achieve strong security.Recentry,KDM security is recognized as a important security,and it's shown that one FO conversion do not have KDM security and another has KDM security.So, we show the other one has KDM security.
Yoshifumi NAKAYAMA	Tsutomu MATSUMOTO	Electrical Security of In-Vehicular Network	Recently, vehicles have been adopted information technology and automatic driving technology receives a lot of attention. On the other hand, the possibility increases that vehicles become the targets of cyber-attack, because they are electronically controlled and connected to the Internet. Therefore, automotive security is needed. In particular, CAN (Controller Area Network) is widely used for the in-vehicle network. This paper points out the threat of Electrical Data Forgery, which focuses on electrical signals of CAN, and discuss the countermeasures against this attack with proposing original method.
Tomomi NISHIZOE	Katsunari YOSHIOKA	Understanding DRDoS Attacks: An Improved Observation Method and Victim Analysis	DRDoS attacks have become a serious threat on the internet since 2013. It is important to understand real-world DRDoS attacks in order to confront them. In this study, we improve DRDoS honeypot which allows third parties to observe DRDoS attacks and analyze victims of DRDoS attacks. First, we propose a protocol-agnostic DRDoS honeypot. Next, we investigate special DRDoS attacks which bypass CDNs and target original web servers directly.

Masato NISHIYAMA	Takashi TOMII	Evaluation of Usefulness of Electric Energy Distribution Based on Context Segmentation of Energy Lifelog	Due to the growing demand for social power reduction, office and other business departments do not impair work productivity, and there is a demand for reduced electricity usage according to the situation. On the other hand, with the development of sensor technology in recent years, the life log on power use can be acquired. So we saved the above logs in the DB and built a system to visualize the power consumption by searching and consolidating power with the situation as the key. In this paper, we propose an electric energy distribution that can intuitively grasp how to use electric power according to the situation by using the above system, and demonstrate its usefulness by quantitatively deriving the effect as the reduced electric energy.
Koya HARADA	Katsunari YOSHIOKA	Detecting Malicious Domains Using Integrated Malware Analysis Service	In recent years, malware carrying out malicious activities that use DNS communication is increasing. Measures such as made to the blacklist are being done but Due to the increase of malware, it is becoming difficult to update quickly. In this paper,We proposed a method to detect malicious domains early and extract them automatically using integrated malware analysis service.
Daiki HIRAKAWA	Naoyoshi TAMURA	Coreference Resolution of The Characters in Novel Text	Characters are represented by various words in novel text. In our research, coreference resolution of the characters in novel text is studied. We propose a model which can deal with same referent of different surficial representations. We propose coreference resolution that consists of three methods, i.e., surficial representation resolution, anaphora resolution and coreference resolution of speaker of uttrance. Considering difference between descritive passage and uttrance,we redefined exophora that related the speaker of the uttrance. By experiments, our method is shown more precise.
Satoshi Hojo	Katsunori Okajima	Crossmodal Effects of Modified Dynamic Visual Information on Beverage Perception	We conducted psychophysical experiments to investigate how visual information effects flavor and impression of beverage. We developed an image processing system adds virtual steam and visual thickening based on the information of the AR marker. By presenting the image processed in real time to the subject with HMD, participants felt that the impression and the flavor changed.

Tatsunori Honda	Toshiyuki GOTOH	A method of Acoustic Output Based on Just Intonation For Virtual Orchestra	We propose a method of performance expression based on just intonation which is a kind of musical temperament. Just intonation has a feature that the frequency ratio is positive integral ratio. Thus just intonation is harmonized. We have studied a method of acoustic output that melody in equal temperament and accompaniment in just intonation corresponding to hearing ability of modern people. In addition, the difference between the note value of the melody in the song and the note value of the accompaniment uses a vibrato corresponding to where the beat occurs. A prototype system with the above requirements was prepared, subjective evaluation experiments and system evaluation were carried out
Atsushi YAHATA	Katsunari YOSHIOKA	SandVeil: A Tool for Improving Sandbox Resilience to Evasion	Recently, Malware, highly functional and malicious software has close connection to many security incident and people need a measure against them. For anti-malware measure, we use sandbox to malware dynamic analysis or detection, but attackers equip a function for evading or obstructing analysis malware. In this study, we suggest a tool, SandVeil, a tool for improving sandbox resilience to evasion by making sandbox environment similar to user machines' one and changing sandbox inherent features.
Akira YOKOYAMA	Katsunari YOSHIOKA	A Study on Detection of Security Inspection System Based on Inherent Feature of Analysis Environment	In this thesis, we introduce SandPrint, a tool that measure characteristics of sandboxes. We collected information from real operation sandboxes using SandPrint to find out the characteristics of sandboxes and verify the possibility of sandbox evasion. We found these sandbox-inherent feature are quite effective for sandbox evasion.
Takahiro YOSHIZAWA	Junji SHIKATA	Unconditionally Secure Searchable Encryption	Searchable symmetric encryption (SSE) enables a user to encrypt data so that the data can be searched without leaking any information on the data. SSE has been studied since the 2000s. However, all existing searchable encryption schemes are computationally secure. Therefore we propose unconditionally secure SSE for the first time in the world. Our SSE scheme is secure against any computationally-unbounded adversary. In particular, we formalize a model and three security notion of SSE and propose constructions which satisfy security definition and derive a lower bound on the secret-key size.

Ryosuke Yoshizumi	Katsunori Okajima	Study on Effects of Spectral Distribution and ipRGC response on Material Perception using a Multi-Spectral Light Source	Light is a critical factor to derive visual information of objects precisely. In the present study, observers subjectively evaluated freshness and glossiness of objects which was illuminated by a light with one of various spectral distributions generated with a multispectral light-source. As a result, freshness and glossiness depend on the spectral distribution of light of which the chromaticity is identical. The results of data analysis indicate that ipRGC outputs contribute to material perception.
Shota YOSHIDA	Tomoharu NAGAO	Destination Prediction for Large Cargo Ships	Multi-agent simulation is widely used for analysis of the various phenomenon of the real world. Prediction of cargo ships' behavior is useful for Shipping company's decision making. In this paper, we construct behavior models of large cargo ships using probabilistic models. The models are constructed with actual voyage data and shipping market data for large cargo ships. We evaluated proposed models by predicting destination of actual cargo ships. By analyzing the experimental results, we considered what information is useful for destination prediction for large cargo ships.
Naoki Watanabe	Tsutomu Matsumoto	Dynamic Call Method: Tamper Resistant Software Using Dynamic Instruction Call Programming	In recent years, Embedded devices used security features are implemented in software. Security features itself need have also be resistance to attacks. In this research I two make proposals. First proposals, I propose method to do self integrity verification with easy restriction which use tamper-resistant-software's parameter stored in hash-table. Second proposals, I propse method to expand the range of system that can be tamper-resistant by dynamic instruction call method. In this paper, It describe proposed method's overview, Implementation procedure and evaluation.
Katsutaka WADA	Tomoharu NAGAO	Emotion Measurement using a Depth Camera	In recent years, researches on emotion estimation to estimate human emotions have been actively conducted. In this research, we focused on puzzled emotions and aimed at estimating puzzled state from a puzzled expression that appears naturally. Based on the opinions of brain scientists, natural puzzle expression evoked experiments were conducted and data on natural puzzle expression was collected from subjects. We also performed classification experiments on puzzled facial expressions on collected data using SVM and estimated puzzle states by combining SVM and emotional transition models.

Yuki MIKI	Tomoharu NAGAO	Construction of stock trading strategy by Deep Reinforcement Learning	In this paper, we propose a construction method of stock trading strategy using deep reinforcement learning.With deep reinforcement learning, it is possible to learn behavior rules that maximize future rewards from past experiences without teacher even if the input is high-dimensional. In this method, we learn a trading strategy that maximizes profit ratio from time series data such as stock price. Furthermore, we construct a trading strategy including optimization of the number of traded shares rather than a simple trading strategy that does not take into consideration the number of trading shares as in the conventional method.
Xinxin XU	Tomoharu NAGAO	CT Image Super-Resolution Using Cellular Evolutionary Neural Networks	Super resolution technology is required for medical images in order to obtain accurate and high resolution images which are easily affected by environmental condition. In this paper, based on Cellular Evolutionary Neural Networks we propose constructing a super resolution processing system that carries out a series of processing including preprocessing of CT images. We reconstructed low resolution images to high resolution images both on the xy-Plane and z-Axis direction. Compared to the results obtained by interpolation based, reconstruction based, and learning based methods, our method gave good results and showed the effectiveness in medical images.