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

Name	Supervisor	Title	Abstract
Jumpei MITA	Junji SHIKATA	Study on Constructions of Key Encapsulation Mechanism from CBDH Assumption	In this paper, we construct Threshold-Tag KEM from CBDH assumption. First, we construct Threshold Tag-KEM from Identity-based Threshold KEM and one-time signature with BCHK transration. Second, we construct Identity-based Threshold KEM from CBDH assumption. This paper first enables to construct CCA-secure Threshold Encryption from CBDH assumption.
Kenta AOKI	Katsunori OKAJIMA	Effect of Stimulus Velocity on Binocular Rivalry	When two unrelated images are presented to left and right eyes, only one of the two images is percepted at a time, and the perceptual dominance is switched in every few seconds. This phenomenon is known as binocular rivalry. The perception alternates between two images at random time, but moving rival stimulus is perceptually dominant over static one. We examined the effects of stimulus velocity on binocular rivalry by varying the stimulus velocity presented to each eye. The results showed that the slower velocity stimuli are perceptual dominant under left-right and expanding-contracting motion conditions.
Hiroshi ABE	Tsutomu MATSUMOTO	A Study on Security of Range Finders	The range-finding system came to be used for a thing about security of the human body such as Pre-crash safety systems of the car. Although considered intentional impersonation or disturbance such attacks classification and countermeasures against it in the measuring system being developed for consumer use has to come done, it leaves much to be desired. In this paper, as an example the typical distance meter as a measurement system was examined on classification of the attack and the measures.

Kento IGARASHI	Toshiyuki GOTOH	Movement Generation of Music Instrument Performance Technique Using the Human Body Model for Virtual Orchestra	In this paper, a method of real time estimation of human joint angle from the positions of figure and arm of human, when playing the musical instrument, is discussed based on inverse kinematic solution, in order to compose the movement of a three-dimensional bone model. Using extended MIDI messages which is embedded as the symbols in staff notations written by MusicXML format, this method enables us to select the playing styles real time during the music performance.
Yuu ISHIDA	Junji SHIKATA	A Study on Constructions of Revocable Identity-based Encryption Secure against Chosen Ciphertext Attacks	we first propose three constructions of adaptively CCA-secure RIBE schemes with decryption key exposure resistance.

Yusuke IMAIZUMI	Tomoharu NAGAO	A Study on Noise Unpleasantness Reduction by Overlapping Sound	Noise reduction methods are important for creating a comfortable sound environment. In this thesis, we propose an unpleasantness reduction method by overlapping control sounds to noises. In our method, control sounds are synthesized from musical sounds whose features are similar to noise. Noises are changed into less unpleasant sound by overlapping them. We evaluated the method by subjective evaluation test. As a result of experiments, we confirmed that our method reduced the sound unpleasantness more effectively than the conventional method based on auditory masking.
Takuya IWAYOSHI	Tsutomu MATSUMOTO	A Study on How to Evaluate Clone Resistance of Artifact-Metric Systems	Artifact-Metrics which is an authentication system to prevent counterfeiting is needed to be evaluated counterfeiting difficulty (Clone Resistance) in variety view points. In this study, I propse new index GSR_{SM} can easily evaluate results even if the conventional index is difficult to evaluate them. And I show efficiency to evaluate and compare some Clone Resistances with use GSR_{SM}.

Akihiro UMEMURA	Tomoharu NAGAO	Creation of the Visual Saliency Map Based on Eye Tracking Data	Modeling human visual saliency has been a very active research field over the decade and many models of visual attention are proposed. There is biologically inspired one to training a model of saliency by machine learning. In this thesis, we propose a method complementing biological model by training human fixations. We evaluated the method by creating saliency map and confirmed that our model is more similar to human fixations than only biological model or training human fixation one.
Marina KASAI	Junji SHIKATA	A Study on Genric Construction of Proxy Re-Encryption	The proxy re-encryption (PRE for short) was proposed by Blaze et al. and it is a public-key encryption scheme having the following useful property.In this paper, we have proposed a generic construction of CCA secure PRE. In addition, we proposed a construction for the threshold hierarchical Identity-based encryption that is a natural extension of Identity-based encryption.

Subaru KAJI	Toshiyuki Gotoh	Using the automotive sensors and 3D-ConstructSystem,Location estimation system of mine locomotive.	The large-sized vehicles which is working in mining environments have a wide dead angle from the driver, and have potential dangers of derailment, a fall, and a collision. Using three-dimensional maps of the haul road, a dangerous position is able to be judged in advance. In this paper, high-speed ICP (Interactive Closest Point) matching algorithm based on Voronoi diagram of the cloud points is first discussed. Then, a method of vehicle location detection in a mining path way using range images observed by on-vehicle camera and three dimensional map of the haul road is proposed.
Natsuko KAWAKAMI	Katsunari YOSHIOKA	A Study on Countermeasures for Targeted Attacks	"In recent years, targeted cyber attacks has become more and more sophisticated. Decoy documents used as camouflage have also become diverse. In this study, we conduct analysis focusing on the contents of the decoy documents displayed at the time of execution of the targeted malware samples. We show that we can often infer the targets of the malware samples from the contents of the decoy document. Also we show that some decoy documents contain confidential information, which implies that the owner of such confidential information may have already been compromised.

Yosuke KIKUCHI	Katusnari YOSHIOKA	Evaluating Security of Android Markets	There are many Android markets all over the world. However, there is a case that market contains malware mixed with regular applications. In order to prevent malware infections, end users should choose safer markets. It is beneficial to evaluate security of markets. In this study, we try to measure the security efforts conducted by market and evaluate security of the markets.
Ryota KIKKAWA	Tsutomu MATSUMOTO	Detection of Targeted Attacks based on Behaviors of Multiple Hosts	Recently, targeted attacks have become a bigger threat. It is important to make countermeasures to detect infected host early on the premise of malware infection, because it is difficult to completely prevent malware infection. One of the countermeasures against targeted attacks is to collect various logs from endpoints and network devices for conducting correlation analysis so as to detect infected hosts. But configuring detection rules suitable for each organization to be protected is still an open problem. In this study, we propose two detection methods of targeted attacks focused on host-based behaviors collected from multiple internal hosts.

Ryota KOIKE	Tomoharu NAGAO	A Study on Feature Space Optimization for Stock Price Prediction	Stock price volatility can be regarded as time series resulting from a complex system from the interaction among market participants. In this thesis, an alternative method to the phase space in the chaos analysis to deal with the complex system, the embedding of the feature space. In our method, we aim to make higher accurate prediction stock price using the feature space than the phase space. As a result of experiments, our method showed that the possibility of performing a more accurate prediction than conventional method.
Takashi KOIDE	Katsunari YOSHIOKA	A Study on Detection and Classification of Malicious Communication	Malicious activities on the Internet have been serious and diverse threats recently. As a countermeasure, observing malicious communication and grasping the reality of the attacks are required. First, We propose a technique for detecting such packets by generating signatures consisting of sequence number in the TCP header, ID in the IP header, ID in the DNS header, and so on. Second, we design and deploy honeypots that observe TCP-based reflection attacks, and confirm TCP-based reflection attacks are indeed conducted in the wild. Finally, we observe the darknet that DRDoS packets reach due to the characteristic IP address.

Tetsuya KOSASA	Tatsunori MORI	A variable-length word N-gram frequency calculation method in large-scale Japanese corpus using parallel and distributed processing	In natural language processing for Japanese, one requires information of frequencies of variable-length word N-grams that can be used to obtain frequencies of N-grams of arbitrary length depending on the situation. However, when calculating the frequency information for a large-scaled Japanese corpus by using existing methods, it is difficult in terms of the time and space complexity to calculate the information with limited computational resources because of the combinatorial explosion of words. Therefore, we propose a method to calculate the frequency information of variable length word N-grams in a large-scaled Japanese corpus by using parallel distributed processing schemes.
Yuuki KOBAYASHI	Tsutomu MATSUMOTO	A Study of Vulnerability Testing Methods for In-Vehicle Network	In the modern automobile, there are many of embedded computers what are called ECU (Electronic Control Unit) to control the automobile. They communicate each other through the in-vehicle bus network realizing the ordinary CAN (Controller Area Network) protocol, for example. I propose methods for vulnerability testing against ECUs connecting to CAN, and make it sure that the methods are effective to test vulnerabilities by putting the test of an ECU connecting to CAN into practice. And, I consider whether one of the methods of vulnerability testing that I proposed can be an attack to an existing protection method for CAN.

Kazuma SASAKI	Minoru SHIRAZAKI	Large-scale parallel analysis for jumping motion of self-propelled fish near water surface	Swimming and jumping motion of aquatic animals is very interesting and remains mysterious in some respects. To unravel mysteries about it, flow around a swimming and jumping fish near water surface is investigated from the view point of computational fluid dynamics with high performance computing to handle large-scale problems. It shows that there is a large connection between waves on water surface and swimming velocity of fish. Especially in cases of swimming near water surface, fish swimming at different velocities generate waves of different patterns. It also shows that swimming with jumping is possibly more efficient than just swimming close to water surface.
Kenichi SHIBAHARA	Katsunari YOSHIOKA	A Study on Analysis of Malicious Networks by Active Monitoring	Attackers compromise hosts and use them to attack others gaining resources for cyber-attacks. Therefore, understanding these resources is important to tackle cyber-attacks. In this study, we analysis these attackers' resources by active observation. Exploit Kits are heavily used to construct malicious web sites for Drive-by Download. We propose a technique to automatically generate signatures to detect Exploit Kits by actually creating malicious web sites using the Exploit Kits and accessing them. And, we define the networks with hosts listing on a lot of ports as malicious network. Using this feature, we propose a method for efficiently finding malicious network.

Takahisa JIN	Tatsunori MORI	Study on Combination of Extractors in Hierarchical Named Entity Extraction	In existing studies of the named entity extraction, embedded named entities, which are contained in other named entities as constituents, are not taken into account when the named entities are compound words. If, however we can extract such embedded named entities, those are useful in question answering, important sentence extraction, and so on. Hierarchical named entity extraction, which is a method to be able to extract embedded named entities in longer named entities, have been proposed. In this study, in hierarchical named entity extraction, we examined the effect of the strusture of hierarchy of embedded named entities and the order of extraction.
Aito SUZUKI	Tatsunori MORI	Study on methods to divide utterance contents of a minutes and link them to a comprehensive plan for political information systems	Since information of regional assemblies is less than that of the National Diet, we study political information systems that show useful information in regional minutes in order for users to make political decision. In this paper, we discuss how to show utterance content in minutes according to the political interest of users. First (1) each of utterances is divided into subparts in a topic-by-topic manner because it usually contains more than one topic, then (2) they are linked to the comprehensive plan of local government. Experimental results show that clue expressions specific to minutes and the topic information in a comprehensive plan are effective.

Shogo SUZUKI	Katsunari YOSHIOKA	A Study on Observation of Attacks Targeting Embedded Devices	It is known that many embedded devices are vulnerable to simple intrusion attempts and it is a serious problem that these devices are abused by various cyberattacks. In this study, we propose IoTPOT, a novel honeypot to emulate services of various embedded devices to analyze ongoing attacks in depth. With this approach, during 263 days of operation, we observed 5,234,103 download attempts of malware binaries from 145,814 visiting IP. By analyzing the observation results of honeypot and captured malware samples, we show that there are currently at least 6 distinct DDoS malware families targeting Telnet-enabled embedded devices.
Daiki TSUCHIYA	Tomoharu NAGAO	Evolutionary Feature Extraction for Image Classification using Genetic Programming	This paper presents an evolutionary feature extraction method for image classification. Our proposed method constructs image pre-processing using graph-based genetic programming, and then selects feature extraction procedures for pre-processed images in evolutionary processes. Subsequently, classification processes are executed using feature vectors that are composed of extracted features from pre-processed images. In texture classification and scene classification problems, it is shown that our proposed method is comparable or better than previous methods. Furthermore, we confirmed that the proposed method can select appropriate feature extraction procedures in response to classification targets.

Takuya TSUTSUMI	Katsunari YOSHIOKA	Understanding Cyber Attacks by Active and Passive Monitoring	In recent years, cyber attacks on Internet have become diverse and serious. In this paper, we summarize our two research achievements that we observed and analyzed on Cyber Attacks by active and passive monitoring for grasping Cyber Attacks.
Shinichiro TOMITA	Junji SHIKATA	Sequential Authentication Codes with Information Theoretic Security	Sequential aggregate signature (SAS) schemes provide a single, compact signature, which is generated from a number of signatures, that simultaneously ensures that each signature is legally generated from the corresponding message with a defined order. In this paper, we first propose sequential aggregate authentication codes (SAA-codes), which has similar functionality of SAS in the information theoretic security setting. Specifically, we give a model and security formalization of SAA-codes, derive lower bounds on sizes of secret keys and authenticators required in secure SAA-codes, and present two kinds of optimal constructions in the sense that each construction meets the lower bounds with equalities.

Masahiro NISHIZAWA	Katsunori OKAJIMA	Projective-AR System for Evaluating Visibility of 3D Package Design	In recent years, it has been required to be considered universal design (UD) in product packaging. However, the evaluation of UD should be spent a lot of time and energy for using some of the elderly and color deficient observers etc. In the present study, we developed a projective-AR system that enables us to simulate appearance seen by persons who have different visual characteristics from young color normal observers by projecting the simulated packaging image to the mock-up in real-time.
Naoki NISHIMOTO	Takashi TOMII	Construction of a Database capable of Electric Evaluation of Each Situation with Micro Data of IoT and Application Method to Smart Grid	Recently, renewable energy such as solar and wind are introduced. Micro-grid is a small power grid that incorporates solar power system at home, office and school, is studied. In this paper, we constructed of a database that integrates daily life log and Open Data. By using this, we assumed the micro-grid that is composed of solar power system and electric vehicles, and derive the power peak suppression effect.

Takuto NISHIYAMA	Toshiyuki GOTOH	3D Shape and Movement Detection Method of Objects Using Moving Stereo Camera	Range images are widely applied to various fields, as the progress of 3D sensing devices. The technologies to analyze individual moving objects are desired to be developed. In this paper, a method to discriminate image regions of moving objects, while removing failure detected motion vectors and effects of the other objects, is first proposed. Then, a method to improve the accuracy of object extraction is discussed, using the probability fields which is represented as the correspondence of objects between subsequence frames.
Keisuke HASHIDA	Katsunari YOSHIOKA	A Study on Android Malware Dynamic Analysis using Real Device	In recent years, Android malware is growing rapidly, and advancing sophistication. Possibility of analysis more effective will be able to by making use of the real device to dynamic analysis of malware that the sophistication of their high.The advantage and disadvantage for dynamic analysis in the real device on the Android malware, were subjected to construction of analysis environment based thereon in the present study.Further, in order to show the effectiveness of the analysis environment using real device, we analyzed same malwares on the emulator. In addition real device and we compared those results and showed the effectiveness of the analysis environment on the real device.

Yuri HIROKANE	Tomoharu NAGAO	Human Attribute Classification Considering Relations among Body Parts	Recently, human attributes such as gender, hair styles, and clothes in images have been used in various fields. In particular, suggestions of pedestrian attributes to a driver are needed toward automated driving in 2020. In this paper, we created a dataset that has four pedestrian attributes - “is male”, “is careless”, “has bag” and “has assisted instrument”- and perform classification of them. Then, we use body parts to adapt to different orientations and shielding of the person, and recognize as human recognize attributes by considering the relations among body parts and obtaining the outputs with numerical values.
Ryota FURUNO	Tomoharu NAGAO	Gradient-Based Feature Optimization for Object Recognition	In object recognition by machine learning, it is necessary to design effective features according to target objects. In this thesis, we propose a feature optimization method based on image gradients for object recognition. The proposed method optimizes a combination of reference regions for extracting features and direction components of gradient histograms used as features by Genetic Algorithm. The experimental result of object recognition shows that low dimensional features acquired by proposed method archives a preferable performance with low computational costs.

Wataru MAEHANA	Tomoharu NAGAO	A Study of Accuracy Improvement of Patient Setup in Image Guided Radiotherapy by Image Processing	A coincidence of center of radiation field (radiation isocenter:RI) and x-ray imaging device (imaging isocenter:II) is important for image guided radiotherapy. Furthermore, to improvement of patient setup accuracy, reduction of an obstacle shadow from x-ray images is required for visual evaluation by medical professional. However, the technique to evaluate a coincidence of RI and II in one sitting is not established. In addition, the x-ray images include the obstacle shadow. In this paper, we developed the evaluation phantom of a coincidence of the two isocenters and proposed image processing method to reduce the obstacle shadow from x-ray images.
Matsui Hyogo	Mori Tatsunori	Answer generation method for university entrance examination in question answering system	We propose answer candidates narrowing method using question focuses we called domain-limited-question-focuses that are more detailed than conventional question focuses and scoring method using distance between answer candidates and attention phrases in factoid type question answering for university entrance examination. As a result of experiment, precision of answer candidates narrowing improved by using domain-limited-question-focuses. And correct answer rate of answering university entrance examination improved by using scoring method we proposed.

Takuya YAMAZAKI	Katsunori OKAJIMA	Study on Recording and Reproducing Methods of Tactile Texture Using a Haptic-Feedback-Device	In human tactile sense, several kinds of physical quantities are intricately involved. For recording and reproducing tactile sense, what we measure and how we translate those should be clarified. In the present study, we propose a reproducing method of tactile sense, such as hardness-softness and roughness-smoothness by measuring physical quantities. We used a PHANToM as Haptic-Device. First, participants adjusted PHANToM parameters so as to match tactile sense to real objects. Next, we measured pressure and shear forces of objects and, formulated the relationships between the physical quantities and the PHANToM parameters. As a result, this system enables us to reproduce tactile sense from physical quantities directly.
Kota YOSHIMOTO	Takashi TOMII	Improvement Accuracy and Verification the Database of EV Energy Consumption Log used by Map-Matching	We constructed a database to store driving energy estimated from driving logs under the assumption if an existing vehicle would be replaced with EV. In this study, we describe the acquisition of the correct data for evaluation this ECOLOG system, the method to improve estimation accuracy and the evaluation method of estimation accuracy. And also describe the error cause of estimated energy consumption.

Miki YONEZAWA	Katsunori OKAJIMA	Effects of Color Distribution on the Impression of Facial Skin	We conducted psychophysical experiments to investigate how color distribution effects impression of facial skin. We investigate how the size of human skin color distribution affects to the facial skin by modifying the size of color distribution and we generated visual stimuli that have different color distribution size. Participants were asked to rate each image from the view of an item. We found that optimal skin color distributions for perceptual human skin's appearance exists but the size of the optimal color distribution depends on the estimated item of skin quality.
Mitsuki Watanabe	Toshiyuki Gotoh	Elastic Matching using NMI and Application to Multimodal Registration	In this paper, the problems of NMI(Normalized Mutual Information), which is applied to matching for deformable objects, are first discussed. NMI is more sensitive to local information than previous similarity values such as ZNCC(Zero-means Normalized Cross-Correlation). We focus on signal to noise ratio based on window size. Then, we propose a new method of registration which is applicable for deformable organs in multi-modal images. Finally, the experimental results are shown, in order to evaluate the effectiveness of our method.

Entei KYO	Katsunori OKAJIMA	Markerless Projective-AR System for Customizing Food Environment	Deliciousness of the dishes cannot be only determined by taste or smell of the chemical attributes of food itself. Food appearance and environment make a great contribution to it. because when given a choice of food, we offen choose to eat what is appealing to our visual appetite. Therefore, if the effects of the appearance of dishes on the visual palatability can be clear, it will be applied to appetite improvement etc. In the present study, we propose a projective-AR system which can modify the visual appearance of the food and dishes in real-time.
Su Jiawei	Yoshioka Katsunari	Detecting obfuscated suspicious JavaScript based on information-theoretic measures and novelty detection	The malicious JavaScript is a main medium for computer network attackers to launch popular Drive-by-download attacks. In this paper, we propose two light weight filter systems for detecting obfuscated malicious JavaScript, which improves several critical potential weaknesses of previous analogous systems.

Do Thanh Long	Junji SHIKATA	A Study on Hierarchical Group Signatures	The group signature scheme has the functionality of the digital signature scheme with the additional property that privacy of signers is protected. Unlike the traditional group signature in which there is only one group manager who manages the group, there is a group signature scheme in which multiple group managers are hierarchically arranged, and it is called the hierarchical group signature heme. However, in the hierarchical group signature, there is no functionality of adding group members. In this thesis, I newly propose a hierarchical group signature scheme in which group members can be dynamically added, and not only the group members but also the group managers can be added in the scheme.
Ching Chze FOO	Katsunori OKAJIMA	Effects of ipRGC Light Responses on Fatigue, Concentration and Arousal Level	We examined the effects of correlated color temperature and the level stimulation of intrinsically photosensitive Retinal Ganglion Cells (ipRGCs) of desk lighting on task performance, visual acuity, physical and psychological effect in Experiment 1. The results show that the lighting with correlated color temperature of 4000 K caused eye fatigue when performing visual tasks as compared to 6200 K. In Experiment 2 and Experiment 3, the results of our studies indicated that the amount of light response of ipRGCs significantly affect physical and psychological conditions of observers, especially on eye fatigue and concentration.

Yun Zhang	Roger Martin	FAKE POSSESSIVES IN MANDARIN CHINESE	This study of Fake Possessives (FP) in Mandarin Chinese shows that the FP can be understood under particular syntactic possessive patterns. I propose the syntax-semantic hypothesis for this phenomenon, which accounts for how the possessive structure corresponds to its non-possessive meaning. Also, built on the experiential study of a number of properties of FP, this analysis explains the distribution of well-formed FP, excluding impossible FP constructions. Furthermore, a comparative study of FP among Japanese, English and Chinese shows that these languages have similarity of subjective interpretation in FP, while they differ in available syntactic structures.