List of Dissertation Abstract (Department of Information Environment)

Name	Supervisor	Title	Abstract
Matsusaki Taichi	Okajima Katsunori	Development of MR character input interface with both fingers	In Mixed Reality (MR) using HMD, character input using a virtual keyboard has become the mainstream. However, there are various problems such as limitation of the field of view and arm fatigue. The purpose of this study is to solve such problems, to develop an interface for hiragana input that is easier to use, and to examine the usefulness of this interface. This interface enables hiragana input by touching the fingertips of the right hand with the fingertips and finger joints of the left hand. We compared the usability of the interface we developed with that of a virtual keyboard in an experiment assuming a situation requiring forward attention. The results showed that the interface developed in this study has higher usability than that of a virtual keyboard.
Ishikawa Yuya	Tomoharu Nagao	Visualization and Analysis of the Condition Transition of CKD Patients Based on the Fluctuation of eGFR	Recently, the number of patients with chronic kidney disease (CKD) has been increasing, and there is a need to elucidate the progression of symptoms and predict future severity of the disease. Conventional studies that analyze symptoms by clustering patients are not suitable for detailed analysis of individual patients because the analysis is performed on a cluster basis. In this paper, we propose a method for visualization of the progression of a patient's condition based on changes in eGFR, a severity index of chronic kidney disease, and a method for evaluation of the progression of that condition. Experiments were conducted to verify the effectiveness of the proposed method and the accuracy of the prediction of eGFR after one year.

Ishida Masaki	Mori Tatsunori	Collecting and Detecting Verbal Irony for Generating Sarcastic Contexts Focusing on Conversation Thread	Utterances on microblogs such as Twitter often lack context. We collected conversation data, considering verbal irony with ironic intent within the utterance itself and its context as appearing in a series of conversations. Further improvements were found in the collection method, such as how to specify queries. Additionally, we created a classifier to detect verbal irony from the collected conversation data. While the classification results were generally good, analysis of misclassified data revealed issues with unconscious human context completion affecting labeling. In order to extract higher-quality verbal irony, it is deemed essential to interpret the meaning solely from the literal information.
Inazawa Tomoya	Yoshioka Katsunari	An Empirical Study on the Usefulness of Security Diagnostic Service for IoT Devices	For a few years now, many consumer IoT devices have been exposed to the Internet and regularly get infected by malware. Thus, the owners' engagement in mitigating IoT-malware-related risks has become a critical challenge, but they may lack information about what they need to do. In February 2022, we launched a web service that allows users to diagnose their devices and check measures as necessary, and we have provided it to 100K general consumers. This paper reveals the high usefulness of the service through user studies and data analysis.

Iwahashi Akira	Tsutomu Matsumoto	Construction of Clone-Resistant Nano Artifact Metric Systems	Artifact metrics is a technology that authenticates artifacts using their unique physical features, and is expected to be "clone-resistant," meaning that it is extremely difficult to create another object (clone) whose values are measured to be equivalent to those of the real thing. In this paper, we propose a new matching method and image preprocessing for "nano-artifact metrics" that use nanometer-scale features, and construct the most clone-resistant nano-artifact metric system.
Iwayama Daiki	Mori Tatsunori	Study of methods for verifying the veracity of secondary information in Japanese assembly minutes	There is a great demand for fact-checking secondary information from assembly minutes. In this study, we examine a method for verifying the veracity of answer summary based on the question summary, the original answers and related information from the question-and-answer sessions in the minutes. We conducted experiments using Large Language Model (LLM), focusing on the format of prompts and the related information utilized. In the experiments, a method that integrated the results of the two tasks demonstrated effectiveness: Recognizing text entailment task between the answer summary and the original answers, and another for determining the relationship task between the answer summary and the question summary.

Uchikoshi Amane	Tsumomu Matsumoto	A Study on Authenticating Avatar Operator and World in Metaverse	Metaverse services are provided by various providers. There have been problems with cases where avatars controlled by users have been stolen by third parties in metaverse services, and cases where fake worlds of user-created worlds have been created to deceive visitors. In this paper, we propose a method that uses biometric authentication to authenticate users and their avatars, and a method that allows world visitors to verify the legitimacy of worlds, while taking into consideration the psychological burden on users who use the metaverse service.
Uchida Yoshihide	Mori Tatsunori	A Study of Learning Data Augmentation methods for Automated Short Answer Scoring	In recent years, the importance of descriptive form examinations has increased, drawing attention to automatic scoring. However, securing learning data has been difficult, and research using a small amount of data has not yet achieved high-precision scoring. We have tried a method of generating new answers through back translation and rearranging and combining phrases from existing datasets. Training with data generated by the proposed method has confirmed improvements in scoring accuracy, and it also suggests the potential to solve the issue of overfitting, where the model learns the position of sentences rather than their meaning.

Endo Yuki	Yoshioka Katsunari	Analyzing the activities of attackers controlling IoT botnets	In recent years, cyberattacks by IoT botnets have become a major threat, and it is important to understand the behavior of the attackers operating them in order to take countermeasures. In this study, we propose a method to identify C&C servers using machine learning from communication during dynamic analysis of IoT malware. We will also analyze the attack infrastructure and attack activities of IoT botnets based on information obtained from continuous C&C server monitoring, honeypots, and dynamic analysis results.
Ohashi Shunsuke	Matsui kazumi	Fatigue Damage Estimation of Curtain Wall by Frequency Domain Method	In order to quantitatively evaluate the fatigue strength of curtain walls, a structural analysis was conducted using variable wind pressure as an external force to obtain local stresses and fatigue estimation. In the case of random vibration such as wind, the fatigue evaluation in the time domain may show a more dangerous side than the actual one unless a sufficiently long time series is used as an input. In this study, the stress time series were converted to stress power spectral density and fatigue estimation in frequency domain method was performed to investigate the trend of the method and its dependence on the selection range of the time series.

Ohara Hirotsugu	Mori Tatsunori	Comparison Study of Performance in Dialect Translation Task Using Unsupervised Text Style Transfer Methods	Appropriate control of the response dialect of a chatbot system can help the system achieve more natural and friendly conversations. We focused on unsupervised text style transfer and examined several methods, including a supervised method, for generating dialect translation models from text data with a specific dialect by deep learning, comparing the kind and amount of data used. Experimental results showed that the method of generating pseudo parallel data using back translation showed high performance comparable to the supervised method, and Few-shot learning using ChatGPT is the most effective when the amount of data is limited.
Ogasawara Takumi	Shushi Harashita	Superspecial Genus-4 Double Covers of Elliptic Curves	We study genus-4 curves obtained as double covers of elliptic curves, called DCEC's for abbreviation. Firstly we provide explicit defining equations of such curves with explicit criterion for whether it is nonsingular. Secondly we enumerate the isomorphism classes of superspecial genus-4 DCEC's in small characteristic p (more precisely p is less than or equal to 23). We accomplish this by implementing our algorithm in the computer algebra system Magma and executing it. Superspecial curves are also expected of the application for cryptography and coding theory, as well as moduli space of polarized abelian varieties in algebraic geometry.

Kashiwagi Keigo	Katsunori Okajima	Computational model of color constancy based on color transparency and color adaptation	Color constancy is a phenomenon in which the color of the same object can be perceived as the same color under white illumination even if the illumination changes. Although adaptive models exist that predict color constancy when color adaptation is activated, these models cannot explain instantaneous color constancy. In this study, instantaneous color constancy was tested using two different color matching methods. The results show that partial color constancy is observed in surface color matching under instantaneous color adaptation conditions. We also measured color constancy under color adaptation conditions, and found that color constancy also occurred in Appearance color match, while color constancy was improved in Surface color match. These results can be predicted quantitatively by a computational model based on color transparency.
Kaneko Takumi	Nakamoto Atsuhiro	Orthogonal partitions of an annulus and their graph representation	An orthogonal plane partition R is a partition of a square by parallel and vertical segments such that for any segment s, each of the two ends of s coincides with an inner point of another segment or that of a boundary edge of the square. The contact relation of the segments in R and the four edges of the square S can be represented as an oriented planar quadrangulation with each inner vertex having out-degree 2. On the other hand, it is known that each of such oriented planar quadrangulations has a realization as an orthogonal plane partition. In this paper, we consider an analogy for a rectangular partition of an annulus, and investigate a relation between the contact relation of its segments and oriented planar quadrangulations with a certain out-degree condition.

Kishimoto Yasutoshi	Shirakawa Shinichi	Expressive Local Explanation Method with Neural Additive Models	Local interpretable model-agnostic explanations (LIME) is a local explanation method that explains the reason behind the prediction of black-box models for a given data. LIME employs a linear model as the interpretable model for locally approximating the prediction of black-box models. However, the linear model used in LIME limits the expressive ability for the explanation. We propose a higher expressive local explanation method using neural additive models (NAM) and its improved model with feature selection as the interpretable non-linear models.
Kojima Masahiro	Takahiro Yamada	Analysis of turbulent structures formed inside and outside the urban canopy using modal analysis	In this study, turbulent structures formed inside and outside the urban canopy was analyzed using proper orthogonal decomposition (POD), which splits the data into a low-dimensional basis, for the flow velocity field in a uniformly arranged group of block that reproduces the urban canopy. Flow structures caused by coherent vortices of the turbulent boundary layer and urban canopy were examined. Five reduced order models (ROMs) were generated from the POD modes and the reproducibility of the original flow field by ROMs was evaluated.

Saino Akihide	Katsunari Yoshioka	Analysis of inducements to fake shopping sites via web searches	In this study, by analysing the web access logs of real users, we investigate how users are redirected to fake shopping sites from web searches. As a result, approximately 5% of the search result pages contained the URL of a springboard site that redirected to a fake shopping site. Furthermore, the user behavior before reaching fake shopping sites and after reaching the sites shows that the user was trying to obtain the product and its information and accessed various sites.
Sakata Genki	Shirakawa Shinichi	Gesture Generation Model with Information about Environment Surrounding Speaker	Gesture generation models take speech information, such as speech audio and speech text, and information about the speaker as input and output gestures. Human gestures are considered to be influenced by the environment surrounding the speaker, such as the position of the monitor. However, because existing gesture generation models do not take such environmental information into account, it is difficult to generate gestures that are appropriate to the environment. This study proposes the gesture generation model that reflects information about the speaker's surrounding environment in addition to speech information.

Shiraishi Kazuma	Shikata Junji	A Research on Homomorphic Signatures with Designated Evaluator	In a homomorphic signature scheme, a signer can sign a set of messages so that anyone can later compute a function of the signed messages and obtain a signature that certifies the correctness of the results. In this thesis, we show that it is possible to construct a homomorphic signature with designated evaluators based on a linear homomorphic signature and a functional commitment with designated openers. We also propose an extension to multi-key signatures. Through our constructions, we obtain a homomorphic signature scheme that supports arbitrary operations based on lattices, and it is shown that the proposed scheme is secure against quantum computers.
Suzuki Yuta	Shirakawa Shinichi	Application of Machine Learning to Neurotoxicity Assessment of Compounds Using Human iPS Cell-Derived Neurons	Neurotoxicity assessment using human iPS cell-derived neurons holds great promise as an alternative method to animal testing. It uses features detected from electrical signals for the assessment. This study proposes a feature extraction method from the electrical signals of neurons. We then assess the neurotoxicity of compounds by machine learning using the proposed features. We analyze the accuracy of each compound and explain the output of the machine-learning model.

Soga Sayoko	Tomii Takashi	Estimation of Energy Conversion Efficiency in Electric Vehicles Using EV Life-Logs	In this paper, we collected and accumulated internal data during the operation of electric vehicles (EVs) as a life log for EVs. Using this data, we estimated the comprehensive efficiency map of the motor and inverter. Furthermore, we utilized the estimated map to perform energy consumption estimation and conducted an accuracy evaluation. This map reveals a breakdown of factors influencing energy consumption, proving to be valuable as a decision-making tool for driving improvements, such as assessing driving speed and acceleration/deceleration methods.
Sogabe Ryo	Morí Tatsunori	Research on Improving Repetition Issues in Generative Task Using Language Model	Since the Scaling Law was proposed, language models have become larger in scale, but in social implementations, lightweight and high-performance language models are in high demand from the viewpoint of cost-effectiveness. In the generation task using such language models, there is a phenomenon in which the same words and sequences are repeatedly generated. In this study, we approached this problem from the aspect of label balance of training data, and were able to show results that improved the repetition problem in generative summarization.

Takagi Yuma	Nagao Tomoharu	Proposal of melody arrangement method through latent space by VAE	In automatic composition, there is still room for research on how to control the music generated. In this paper, we propose a method to change the tune of a piece of music. In this study, the rst target is time signatures, and the goal is to arrange a 4-beat song into a 3-beat song. The proposed method rst acquires a 2-class classi er that determines whether a song is in 3 or 4 beats, and then performs ne tuning of the learned VAE to generate a melody that the classi er determines to be in 3 beats. Subjective evaluation con rmed that the arrangement to 3 beats was achieved while maintaining the original tune.
Takayasu Masato	Nagao Tomoharu	Construction Music-Evaluation-Function Optimized by User Preference	Recently, the copyright of data used for training generative models becomes an issue. In addition, it is concern that the spread of generative models increases the amount of content and demand for recommendation systems. However, existing recommendation methods have the "cold start" challenge. Therefore, in this paper, we propose a music evaluation function optimized by user evaluations as a method to mimic user preference information and to learn models using features that cannot recover the original data. In experiments verify the effectiveness of the music evaluation function in terms of four aspects: lightness, ease of learning, prediction accuracy, and data unrecoverability.

Takiyama Hikaru	Yamada Takahiro	Development of experimental methods in the mechanical evaluation of suture procedures	An experimental method was developed to quantitatively evaluate suture technique from mechanical data. Experiments were conducted using simulated organs instead of organs to simulate actual suturing procedures. We focused on the deformation state of the organ surface as the evaluation index mechanical data, and measured the surface strain of the simulated organ during suture by experiment. In addition, we compared the deformation state when suturing was performed under different conditions to consider the influence of each condition on the deformation state and to evaluate the technique.
Tanizaki Shunsuke	Katsunari Yoshioka	Evaluating the Behavior Detection Functionality of Endpoint Security Solutions against Double Extortion Ransomware	Double extortion ransomware poses a significant threat to both organizations and individuals. This ransomware not only encrypts or deletes files but also exfiltrates them. This study investigates the effectiveness of seven antivirus software and one EDR against double extortion ransomware. We executed ransomware test samples on a machine where the products were installed, and few products were able to detect the behavior of the test samples and prevent them from running.

Chikano Masaki	Tsutomu Matsumoto	A Study on Laser Detection Sensor Implemented on FPGA	Digital sensors have been proposed for detecting laser fault attacks, and one of the digital sensors using a ring oscillator has been proposed. In this study, I show that the laser detection sensor using a ring oscillator proposed in a previous study does not sufficiently detect lasers, and that it does not detect lasers sufficiently when the pulse width and power of the laser are reduced. I also propose an improvement plan and show its effectiveness.
Chiku Sohto	Junji Shikata	A Study on Improving Security of Identity-based Matchmaking Encryption	Identity-based matchmaking encryption (IB-ME) is an encryption scheme that both the sender and the receiver can mutually specify their identities. In IB-ME setting, a third party called a key generation center generates a secret key for each user, which is called the key escrow problem. In addition, almost IB-ME schemes do not satisfy the security requirements for general encryption and signature schemes. In this work, we constructed an IB-ME scheme that handles the key escrow problem and some IB-ME schemes that satisfy strong security.

Tomei Kota	Mori Tatsunori	Construction of a System to Structure and Visualize Accident Cases for Automated Response Generation	In industries such as manufacturing, responding to inquiries about accidents on-site is currently done manually, which is inefficient. Consequently, there is a significant demand for automated response systems. This research aims to clarify the causes of accidents by visualizing and presenting the structured flow of accidents when the system responds. We developed an annotation framework to structure the flow of accidents from plain text and applied it to some cases in the "Failure Knowledge Database" to organize a text corpus. Additionally, we built a system for structuring using GPT-4. Evaluation experiments to measure the system's performance showed that there is room for improvement.
Nakada Yuki	Shushi Harashita	Classification of sextic models of curves of genus 5 with gonality 4	It is known that a curve of genus-5 determined by three 5-variable quadratic equations is birational to a plane curve of degree 6. In this study, we attempted to classify the singularities of that plane degree-6 curve using theoretical and computational methods. Specifically, we used a computer program to calculate the dimension of the space of curves for each type of classified singularity. As a result, we succeeded in determining the dimensions for all seven types of singularities in characteristic 0. Future works would include the calculation of the dimensions for other characteristics.

Nakanishi Ryo	Tomoharu Nagao	Optimization of Cultivation Conditions in a Plant Factory Based on Human Knowledge	Artificial light type plant factories can precisely control various cultivation conditions and stably grow plants. However, the cost is high and the profit is low compared to the cost. In this paper, we propose a method for finding cultivation conditions that increase the growth rate of plants to improve profitability. The proposed method compensates for the small number of cultivation data by using constraints based on human knowledge that has been collected and analyzed in advance. As a result of applying the proposed method to cultivation data, we found cultivation conditions that are expected to be a higher growth rate than before.
Nishimura Rei	Nagao Tomoharu	Enhancing characteristics of 3D motion with text	Today, human 3D models and 3D motion are being studied and utilized in various fields. Many AI models are also studied that enable users to easily generate 3D motion from a small amount of input, without the need for advanced technology or expensive equipment. For them, I propose a method of creating a text dataset that acts on the training of models that generate 3D motion from natural language text as input and enhances the motion characteristics of the generated motion.

Ninomiya Sota	Fujii Tomohiro	Model construction and comparison of competing hypotheses for the English interrogative sentence formation rule: A Bayesian approach	We constructed a Bayesian model for hypothesis acquisition of the English interrogative sentence formation rule and quantitatively verified hypothesis acquisition. This model evaluates the trade-off between simplicity of transformation rules and goodness of fit to the corpus of mostly child-directed utterances that we used. Transformation rules can fall into two categories: "linear" or "structural," depending on the type of representation they are built on. Experimental results showed that linear rules are superior in terms of simplicity. Furthermore, it has been suggested that by using adult utterances from the real corpus, children can learn the structural hypothesis according to which the main-clause auxiliary verb must be fronted, which is actually used by English speakers.
Hashimoto Shunki	Okajima Katsunori	Simulation of DoF blur considering vergence characteristics of HMD wearing and its application	When the vergence distance is measured from the viewpoint position during VR observation, there is a "gap" between the distance to the gazing point and vergence distance. In this study, we developed a method to obtain the distance to the gazing point in the virtual space by correcting the vergence distance, and developed a VR system that adds appropriate DoF blur. To confirm the usefulness of this calibration system, we conducted experiments in a VR environment and a real environment. The proposed vergence distance correction system reproduced a view closer to reality than the conventional VR environment without DoF blur.

Hiroi Tatsuki	Tomii Takashi	Multi-Faceted Quantifying for the Introduction Effect of a Smartgrid Using Load Leveling Oriented VGIDB Integrating PV and EV	In this study, we conducted database design and simulations to evaluate VGI (Vehicle Grid Integration), which represents a new approach to integrating PV (photovoltaic) and EV (electric vehicle) systems into a smart grid . In the simulations, parameters such as the number of EVs and the amount of PV installation were considered, and the results were stored in a database for query processing to quantify the introduction effects. By setting multiple evaluation metrics, we demonstrated that the effectiveness increases significantly as both PV and EV increase simultaneously.
fukutani yuki	Yamada Takahiro	Establishment and assessment of credibility for simulation models	This study assesses credibility by quantifying epistemic uncertainty of material models and material parameters identified from material tests, based on the concept of evaluating the credibility of simulation models presented in ASME V&V-40. Using 4-point bending tests on wood as an example, the credibility of the Calibrated material model will be evaluated for those that have only identified the parameters and those that have confirmed the reproducibility of other responses. Validation activities using the credibility-assessed material model were conducted to demonstrate the usefulness of the proposed credibility factor.

Fujimoto Haruki	Junji Shikata	A study on constructing Proxy Re-encryption based on LPN Problem	We propose a proxy re-encryption (PRE) scheme based on the Learning Parity with Noise (LPN) problem using error-correcting codes. Several lattice-based PRE schemes have been proposed as post-quantum PRE. Our proposed scheme is the first PRE scheme based on LPN.In this paper, we construct a LPN-based PRE scheme from a LPN-based public key encryption (PKE) scheme proposed by D"{o}ttling et al. (ASIACRYPT 2012), so that we can apply techniques used in lattice-based PRE and then prove its correctness and CPA security.
Maeda Riku	Okajima Kastunori	Effects of autonomic nervous system modulation on taste perception	The five senses and the autonomic nervous system play a significant role in human behavior, emotions, and health, with taste being particularly crucial in daily life. This study delves into the interaction between taste and the autonomic nervous system by examining changes in taste sensation reported after exercise, exploring the correlation between heart rate and taste threshold. The findings suggest that modulation of the autonomic nervous system likely influences taste perception, based on temporal changes in taste thresholds and physiological responses of the brain and body.

Matsuoka Yoshiro	Junji Shikata	A Study on Message Authentication Codes Capable of Key and Data Compression	In this paper, we propose a new cryptographic protocol called proxy re-authentication capable of key and data compression. In particular, we realize key compression by converting a tag generated with a sender's private key into another one so that a receiver can verify with his own private key through a proxy. Moreover, regarding this protocol, we show that it is possible to realize data compression by aggregating tags based on the idea used in aggregate message authentication. Concretely, we provide two constructions: one is a generic construction using key homomorphic pseudorandom function and the other is based on the hardness of the computational Diffie-Hellman problem.
Matsumoto Yuta	Shinichi Shirakawa	Improvement of Sample Weighting Method via Optimal Transport for Complicated Dataset Shifts	Distribution shifts are problems in which the distributions of the training and test data differ and significantly degrade the performance of machine learning models. Sample weighting methods change the impact of each data for updating the model by assigning weights to data and are effective against distribution shift by giving appropriate weights. This study proposes three im-provements to the existing sample weighting method using optimal transport distance to improve the performance in a complicated distribution shift with mixed label noise and class imbalance.

Matsumoto Ryo	Tomoharu Nagao	Building a Model Simulating Vital Data of Emerging Infectious Disease	Since the recent pandemic of COVID-19, there have been many challenges trying to build a model meeting needs of overwhelm medical field in the midst of an epidemic of emerging infectious diseases. In this paper, we try to build a model that simulates time-series changes in vital data for each patient's prognosis in order to meet every needs with medical concreteness. We propose building a simulation model that utilizes data resources efficiently, and this model may meet every needs relatively well.
Mabuchi Yuki	Shinichi Shirakawa	Creation of SNS Dance Dataset and Its Application to Dance Generation Model Training	To assist choreographers in creating dances, research on the machine learning-based automatic generation of dance that matches a given music has been conducted. Recently, the demand for short and catchy dances on social media has been increasing. However, the dances in the existing datasets for automatic dance generation models are long and contain complex movements. Therefore, generating dances suitable for social media using such a dataset is difficult. This study creates a dataset of short and catchy choreography and evaluates the trained dance generation model using that dataset.

Miyata Hiroto	Tsutomu Matsumoto	Implementation and Evaluation of Pairing Calculations in Resource-bounded IoT Devices	Pairing cryptography is sometimes used for communication between IoT devices, but the core pairing computation is computationally expensive and can be difficult to implement in IoT devices with small RAM capacity. In this study, we propose the use of 128-bit security, based on the fact that 256-bit security is being considered for long-term security in the future. The BLS48-581 curves for 128-bit and 256-bit security, respectively, are used in this study. BLS48-581 curves for 256-bit security, and proposed an implementation for devices with minimal computing resources. We then clarify the relationship between security level and computational cost.
Miyano Kota	Ushikoshi Erika	Asymptotic behavior of the eigenfrequencies of a thin elastic rod with a junction in three-dimensional space	There are many results about the analysis for the eigenfrequencies of homogeneous isotropic elastic body. In the works, Kerdid(1997) studied eigenfrequencies with a joint of two rectangular solids and in recent years, Jimbo-Rodriguez Mulet(2020) analyzed it for an elastic rod with non-uniform cross-section. The purpose of our study is to build the foundation of mathematical analysis for eigenfrequencies of an elastic body with a junction of more general shapes, and we succeeded to obtain the derivation of asymptotic order of eigenvalues.

Murata Motoki	Okajima katsunori	Developed food appearance changing system using a non-coaxial projection camera system that enables 3D tracking and verification of cross-modal effects	Coaxial projector-camera systems are mainly used for dynamic projection mapping that can track three dimensions. However, such a system requires delicate optical axis adjustment. In this study, we developed a dynamic projection mapping system using a non-coaxial projector-camera system that is easy to implement and enables high-precision three-dimensional tracking. Cross-modal effects were verified by manipulating the appearance of food products, by using our system expecting an improved eating experience.
Mori Yuta	Takahiro Yamada	Assessment of Modeling Credibility by Indentation of a Simulated Organ	In this study, an identification method using a minimally invasive indentation test and inverse analysis is developed to obtain the physical properties of inhomogeneous organs. Validation of the property identification method is performed at the homogeneous body level. Indentation test is carried out on a simulated organ made of homogeneous material, and the reaction force and deformation are measured. The material parameter of the simulated organ is identified from the tensile test and forward analysis is performed. The validity of the property identification method is confirmed at the homogeneous material level by comparing the responses between the experimental and analytical results.

Morii Yudai	Yoshioka Katsunari	Analysis of IoT device manufacturers' handling of OSS vulnerabilities	In this study, we applied a Software Composition Analysis tool, which has recently attracted attention as one of the vulnerability management methods, to the firmware of IoT devices, and analyzed IoT manufacturers' handling of vulnerabilities in Open Source Software. As a result, we confirmed that there are differences among IoT manufacturers in their handling of known vulnerabilities at the time of firmware release, and that there are cases in which vulnerabilities increase due to firmware updates.
Yasui Hiroki	Katsunari Yoshioka	Research on Understanding IoT Malware Activities through Attack Observation with Bare Metal Devices	Recent IoT malware has sophisticated functions and the realities cannot be clarified only by dynamic analysis in a virtual environment. In this study, we operated observation systems using actual IoT devices and investigated the actual situation of IoT ransomware and the survival competition of IoT bots. In the former case, we clarified that the operation of the attack infrastructure is automated to maximize profits, and in the latter case, we clarified that the infection status of vulnerable devices varies greatly depending on the time of observation and the characteristics of the devices due to the battle for control by the attackers.

Yoshida Yosei	Nagao Tomoharu	Concept-conditional Synthetic Image Generation with Diffusion Model for Koi Evaluation System	In recent years, the international expansion of the Koi culture has led to the necessity for online appraisal competitions. While online competitions anticipate fair evaluations through machine learning, there is a challenge in securing the substantial amount of image data required for such learning. In this paper, we propose a method to generate realistic and high-quality synthetic image data by learning Koi-specific concepts from known individuals and providing them as conditions. The experiments include qualitative comparisons of generated images and a perceptual quantitative assessment to verify effectiveness and identify useful conditions.
Yoshiya Kazuya	Takahiro Yamada	Splitting Time Integrator for Mixed Finite Element Method in Dynamic Analysis of Beam and Plate	In this work, the mixed finite element method, in which one or both of the transverse shear stress and the axial normal stress are taken as independent variables, is applied to dynamic problems of the Timoshenko beam and the Mindlin-Reissner plate. The splitting time integrator designed for the mixed method, which works as an explicit method for bending deformation and as an implicit method for the others, is adopted. Therefore, the time interval can be determined by the wave velocity of the bending deformation and its restriction is relaxed. The numerical properties of the proposed approach are evaluated by numerical experiments.

Washizu TADAAKI	Katsunori Okajima	Dynamic auditory induced visual image illusion mechanism using color and shape perception	The audiovisual linkage illusion, in which two synchronized lights appear to be three by three consecutive sounds, is an illusion produced by posterior prediction due to cross-modal effects. However, it has been unclear whether this illusion also occurs when the first and second visual stimuli are different in color or shape. In this study, we show that the audiovisual-linked illusion does occur even when the color and shape of the front and rear optical illusions are different, and that which of the two illusions is dominant depends on the individual observers.
HE ZHENYANG	Matsui kazumi	Stochastic evaluation for Stiffness/Strength of Polycrystalline Structures	At present, the destruction caused by the techniques used to elucidate the internal structure of ceramic material is irreversible, making it impossible to verify the original experimental specimen. Therefore, this study applies Voronoi partitioning and infers the internal structure based on information obtained from the top surface of microcantilevers using electron backscatter diffraction. Additionally, efforts are made to develop acceleration techniques (conjugate gradient method) necessary for conducting stiffness and strength evaluations for polycrystalline models.

KHANG MINJE	Shikata Junji	A Study on Improving Efficiency of Searchable Encryption by Using Fast Fourier Transform or Hybrid Sampler	Recent years have seen technological advancements in quantum computers, indicating that many cryptographic algorithms could be vulnerable to attacks by quantum computers. Consequently, cryptographic research into quantum-resistant cryptography has been extensively pursued. For Public Key Encryption with Keyword Search (PEKS) as well, research based on lattice-based cryptography, one of which is the NTRU cryptosystem known for its quantum resistance, has been advancing. However, existing NTRU-based PEKS schemes use a Gaussian sampler for trapdoor generation, which requires $O(n^2)$. This thesis proposes a structure that applies the fast Fourier sampler from FALCON and the hybrid sampler from ANTRAG to improve the trapdoor generation time to $O(n \log n)$ in PEKS. Furthermore, it evaluates and compares the efficiency of these two schemes.
HUANG BEN	Katsunori OKAJIMA	Real Image Substitution for Avatars in Virtual Space Communication System	To enhance the authenticity of communication in virtual reality systems, we propose a new method of transforming avatars into real image by using three cameras. Avatars are rendered realistically, and the new virtual space communication system does not require HMDs. Performance measurements show that the proposed model is capable of real-time processing. Furthermore, the results of evaluation experiments demonstrate that our system provides higher authenticity and immersion compared to traditional communication systems.

XIE NINUO	Nagao Tomoharu	Improving Accuracy in Adverse Image Detection for Image Classification Utilizing Human Rationale	In image classification with Convolutional Neural Networks, the necessity for extensive training data and the complexity of interpreting the model's decision-making process are significant challenges. This paper introduces a methodology aimed at identifying images that could potentially hinder model performance by leveraging annotations related to human decision-making and heatmap analyses. The primary objective is to enhance the model's precision by pinpointing images that evoke divergent opinions among humans, as indicated through annotations, and by identifying images featuring multiple instances of the same object, as revealed through heatmap analysis. This selective removal aims to streamline the training dataset, leading to enhanced model precision and accuracy.
CHEN YEN－HSIU	Shirakawa Shinnichi	Architecture Search of Neural Networks Using Discrete Embedding Representations for Split Inference	Split inference is a technique that divides an AI model and deploys it separately on edge devices and server-side for inference. This approach addresses privacy concerns in cloud computing and reduces high latency caused by transferring large amounts of data. Besides, the data transmission volume and the model's computational cost depend on the model architecture and splitting point. Meanwhile, not all existing models are suitable for split inference. To facilitate the effective use of split inference across various models, this research proposes an automatic architecture search method for split inference, reducing data transmission and the overall latency of model inference.

| Liu Yi | Takashi Tomii | Design of Electric Vehicles' Energy Baseline Maps with Wind Conditions and Accuracy Verification Using Long-Term Driving Data | In our previous study, we proposed electric vehicles' (EVs') Energy Baseline Maps (EBM) that visualize the essential energy consumption explained by road gradients. However, the EBM did not consider the influence of wind. In this paper, we propose an improved version of the EBM, called Energy Baseline Map-Correction of Airspeed (EBM-CA), by enhancing the calculation of air resistance using meteorological open data to calculate the effect of wind. Utilizing long-term accumulated real driving data of EVs, we compared the EBM-CA with the EBM and confirmed the improved evaluation accuracy of the EBM-CA. Furthermore, by visualizing the EBM-CA on a location basis, we demonstrated the impact of seasonal wind on EV energy consumption. |