

No.450



Cover image: Easy Conveyance of Samples that are Sensitive to Air Exposure

Human Brain Regions for Perceiving "Glossiness" Located for the First Time

-Major advance in objective evaluation of surface qualities-



Atsushi WADA Researcher, Multisensory Cogni-

Researcher, Multisensory Cognition and Computation Laboratory, Universal Communication Research Institute

After completing graduate school, worked at the Advanced Telecommunications Research Institute International (ATR), before joining NICT in 2009. Engaged in artificial intelligence, functional neuroimaging, and visual neuroscience. Ph.D. (Informatics).



Yuichi SAKANO

Researcher, Multisensory Cognition and Computation Laboratory, Universal Communication Research Institute

After completing graduate school, he became a post-doctoral fellow in York University in Canada, then joined Cognitive Information Science Laboratories at the Advanced Telecommunications Research Institute International (ATR) before joining NICT in 2009. Engaged in human visual perception and psychophysical evaluation of visual displays. Ph.D. (Engineering).

Hiroshi ANDO

Director, Multisensory Cognition and Computation Laboratory, Universal Communication Research Institute

After completing a doctoral course, joined the Advanced Telecommunications Research Institute International (ATR) in 1992 and worked as Head of Department of Perceptual and Cognitive Dynamics until 2011. He has been involved in NICT's R&D project for ultra-realistic communications from 2006. Engaged in brain and cognitive sciences and multisensory information processing technology. Ph.D. (Computational Neuroscience).

Introduction

The objects around us have different surface qualities due to differences in material (metal, glass, wood, leather, etc.) and surface physical properties (microscopic roughness. elasticity, and light reflectance). We can visually discriminate various surface qualities instantly from our retinal images, but solving such estimation problems is generally difficult without assumptions (such as location of light sources or object shape). This remarkable ability of the human visual system to distinguish surface qualities cannot be matched by the latest computer vision systems. In this research, we have focused on the perception of glossiness (surface shininess), a major component of surface quality, and clarified related neural mechanisms that had been largely unknown before. We used functional Magnetic Resonance Imaging (fMRI) to measure neural activity during glossiness perception and for the first time, successfully identified the human brain regions involved in the processing of glossiness.



Figure 1 Visual stimuli used in experiment 1

Identifying brain areas involved in perception of glossiness

Generally, objects that have highly glossy surfaces generate specular highlights (bright spots) due to the reflections of light sources or the surrounding environment. These features have a large effect on luminance and color, which are basic elements of visual processing. However, many neurons in the visual cortex show simple responses to luminance and color, regardless of glossiness. Therefore, we had to devise a method to separately measure the brain activity induced by the processing of glossiness itself.

In our experiments, we were able to identify neural activity involved in perception of glossiness by combining two methods. One using illumination constancy, a characteristic of human visual perception, in which perception of glossiness remains stable under different lighting conditions (Experiment 1), and another based on visual attention, a neural mechanism that selectively induces processing of the attended visual feature (Experiment 2).

In Experiment 1, images of objects with high and low glossiness placed in conditions of bright and dim illumination were used (Figure 1). We then investigated brain areas where activity increased when the objects with high glossiness were presented, compared to when those with low glossiness were presented, regardless of differences in the level of illumination.

Then, in Experiment 2, we measured changes in neural activity when performing a task of discriminating either glossiness, shape, or orientation of objects, in order to dissociate neural response to simple visual features that happened to covary with glossiness (e.g. changes in color due to highlights, etc.). More specifically, the



Figure 2 Visual stimuli used in experiment 2

subjects viewed a pair of sequentially presented objects (shown in Figure 2) and judged whether the attended visual feature (e.g., high or low gloss under glossiness discrimination task) was identical or not. The measured brain activity was then compared between different discrimination tasks. We examined which areas of the brain had increased activity when attending to glossiness.

The results from both experiments clearly identified multiple brain areas involved in the perception of glossiness, including the hV4 and VO-2 visual areas in the ventral visual pathway, the information processing path from the primary visual area (V1) of the occipital lobe, and the V3A/B visual area in the dorsal visual pathway from V1 to the parietal lobe (Figures 3 and 4).

Two visual pathways and the neural processing of glossiness perception

The ventral and dorsal visual pathways have been suggested to play different roles in the processing of visual information in the cerebral cortex. The ventral visual pathway (the "what" pathway) has been associated with visual object recognition, while the dorsal visual pathway (the "where/how" pathway) with visual spatial processing or that to guide action. It has also been hypothesized that the two visual pathways function independently, because damage to either pathway is known to impair the respective functions. However, the precise roles of each pathway and their independence, which remain important issues in neuroscience, have not been clarified in detail.

Our results have significance in this context, because we showed the involvement of both the ventral and the dorsal visual pathways in glossiness perception (Figure 3). Recent studies on monkeys have reported the involvement of the ventral visual pathway in the processing of glossiness but such involvement has not been reported for the dorsal visual pathway. Therefore, our results suggest that the processing in the dorsal visual pathway for surface quality perception might be human-specific, and may also give implications for understanding how the two visual pathways are functionally organized.

Conclusion

The attractiveness and feel of objects is greatly affected by differences in surface quality, so it is a very important element in industrial design, including architectural (e.g., interior and exterior of buildings), automotive, and product design (e.g., furniture, appliances, and mobile phones). However, it is difficult for individuals to express their perception of surface quality in words. Even if different people use the same words to describe a surface quality, they may not necessarily be perceiving it in the same way. Thus, if we can estimate subjective impressions by objectively measuring the corresponding brain activity, we should be able to understand perception of surface quality in more objective and quantitative ways. This could be used to develop products that appeal to people's sense of high quality and high class. In the future, we plan to further investigate the functional role of each brain area involved in surface quality

perception, not only for its scientific significance, but so we can implement technology to evaluate surface quality, both objectively and quantitatively, from brain activity.

These results were published in the September, 2014 issue of NeuroImage, an authoritative international journal in this area of research.



Figure 3 Neural pathways involved in perception of glossiness (areas shown in red)



Figure 4 Change in neural activity due to high glossiness, as confirmed in experiment 1

SPHERE: A New Encryption Scheme Allowing Both Security Updates and Operations on Encrypted Data



(Front from the left) Trieu Phong LE, Yoshinori AONO (Back from the left) Takuya HAYASHI, Lihua WANG

Trieu Phong LE Researcher, Security Fundamentals Laboratory, Network Security Research Institute

After completing a doctoral course, worked as a researcher at Tokyo Institute of Technology and then joined NICT in November, 2009. Engaged in designing and evaluating of cryptographic protocols. PhD.

Yoshinori AONO

Researcher, Security Fundamentals Laboratory, Network Security Research Institute

Takuya HAYASHI

Researcher, Security Fundamentals Laboratory, Network Security Research Institute

Lihua WANG

Senior Researcher, Security Fundamentals Laboratory, Network Security Research Institute

Background

Various services have been developed with recent developments in data mining technology, but leakage of private information from such data has become an issue. One technique that is receiving attention as a way to resolve this issue is called homomorphic encryption, which allows operations to be performed on data in its encrypted form. By using homomorphic encryption, data can be processed while preserving privacy of the data.

As an example, consider the case of gathering sensitive data from hospitals, such as the state of diseases or genetic data, and using statistical processing to estimate trends for diseases, or to decide treatment methods. It is expected that the amount of data obtainable from hospitals will increase greatly in the future, and large amounts of computing resources will be needed to perform such data mining. Using a cloud service is attractive, considering costs and the need to backup for business continuity planning (BCP), but storing such sensitive data on a cloud server can be associated with leakage of private information. Homomorphic encryption can allow the benefits of cloud infrastructure to be utilized while still preserving privacy (Figure 1).

For a system handling sensitive information such as disease or genetic data, the effects of a data leak can reach not only the individual patient, but also any relatives, so security must be maintained over long periods of time. On the other hand, cryptanalysis and computing power continues to advance yearafter-year, so the security of encrypted data is decreasing. To maintain security over long periods, the security level must periodically be increased by changing the key length. There are two ways to implement key-length changes, as follows, and each has its own short-comings.

- Decrypt the ciphertext and then re-encrypt using a more secure encryption method. This method has the possibility of data leak while the data is decrypted.
- (2) Encrypt the ciphertext using an existing, more secure encryption method without decrypting. With this method, data must be transformed and partitioned, so further data processing is not possible.



Figure 1 Medical information sharing system considering privacy

Figure 2 Example use of the homomorphic encryption method that allows key length to be changed

Accordingly, we have proposed the idea of a securityupdate function to change the key length, distinct from these methods, and developed a new encryption scheme called Security-updatable Public-key Homomorphic Encryption with Rich Encodings (SPHERE). SPHERE is the first ever encryption technology achieving both security-level updating and efficient homomorphic operations (Figure 2).

Updating the security level of encrypted data with SPHERE

Encryption of data with SPHERE was implemented by developing a technique*¹ that partitions the ciphertext into a data region and additional noise, and allows the length of the additional data to be extended securely (Figure 3). The plaintext is expressed as a vector, and the secret key and public key are expressed as matrices. During encryption, additional data is generated using the public key and a noise vector, and the plaintext vector is scrambled using the public key and the noise vector. To decrypt this ciphertext, the corresponding secret key is used to recover the information needed for decryption from the additional data, which is then used to unscramble and recover the plaintext.

To update the security level, an update key is generated from the old secret key and a new secret key with a higher security level. This update key and the new public key are then used to extend the additional information, and by adding a noise vector to further randomize it, the ciphertext security level is updated and increased.

Implementing efficient linear regression on encrypted data with SPHERE

Linear regression is a method used in data mining to estimate an equation for the relationships between explanatory variables and objective variables in the data being analyzed.

The fastest result in existing research to compute linear regression securely using encryption technology is due to researchers from Stanford University and Technicolor Inc.*². This research implemented linear regression by combining a type of homomorphic encryption called Paillier encryption and a technique called garbled circuits. However, Paillier encryption requires handling integers of at least 300 digits, and the structure of garbled circuits is very complex, so it has been difficult to compute quickly, especially when the number of features in the



Figure 4 Comparison with existing research



Figure 3 Overview of SPHERE

data is large.

In contrast, linear regression with SPHERE is implemented by adding and multiplying vectors and matrices of integers of length at most tens of digits, so it can be computed quickly, even on big data sets with numerous features. It can also be parallelized easily, so computing time can be reduced greatly by using many computers at the same time.

When we compared processing times for computing linear regression on the real data set^{*3} used in the existing research described above, SPHERE was an average of 100 times faster (Figure 4). We also confirmed the ability to compute a linear regression on a much larger, synthetic data set of one million records in approximately 30 minutes.

Future prospects

In the future, we want to show that it is possible to build a large-scale, privacy preserving data mining system by performing computations used in fields such as insurance and bioinformatics on encrypted data, on data at a scale of 100 million records, comparable to the population of Japan, and to have such a system used in the real world.

- *1 SPHERE uses a lattice-based encryption technology, the security of which is based on the practical difficulty of computing the shortest vector problem on a lattice. This problem becomes more difficult as the length (dimension) of the additional data increases. Thus, by selecting secret and public key parameters such that the additional data is longer, ciphertext with a higher security level can be created.
- *2 Nikolaenko et al., "Privacy-Preserving Ridge Regression on Hundreds of Millions of Records," IEEE Symposium on Security and Privacy 2013.

*3 UCI dataset (https://archive.ics.uci.edu/ml/datasets.html)

Easy Conveyance of Samples that are Sensitive to Air Exposure

-Introducing a portable ultra-high vacuum (UHV) sample conveyance system—



Shukichi TANAKA

Research Manager, Nano ICT Laboratory, Advanced ICT Research Institute

Completed a doctoral course in 1996. After working as a Research Fellow in the Japan Society for the Promotion of Science, as a Research Assistant and later Associate Professor in the Department of Physics, Graduate School of Science and Engineering, Saga University, and as a Research Fellow in the Department of Condensed Matter Physics, the University of Geneva, joined the Communications Research Laboratory (currently NICT) in 2002. Engaged in development of ultra-fine measurement, nano-process, and molecular nano-device technologies. His specialties are in nanostructure properties, physics of material science, and biomaterials applications. He is an invited Associate Professor in the Graduate School of Engineering, Osaka University. Ph.D. (Physics).

Research overview

Samples whose basic characteristics can be greatly altered by even minute exposure to air must be handled under ultra-high vacuum (UHV) conditions in order to maintain their intrinsic properties. Examples of such materials include structures at nano-meter scale, requiring processing accuracy on an atomic or molecular scale, and material surfaces that greatly influence the performance of batteries, sensors and other devices. To meet these sorts of technical demands, NICT, in collaboration with the Kyushu Synchrotron Light Research Center, Saga Prefecture, has developed a portable lightweight vacuum system equipped with a UHV pump that can operate independently using dry-cell batteries.

Background

When visiting users perform analysis or processing at large shared facilities such as the synchrotron radiation facility, usually samples to be measured or processed are treated and set into the analytic equipment in air, but intrinsic properties of samples with highly reactive surfaces, such as catalysts or sensitive electrodes, can be changed greatly due to contamination and chemical reaction with oxygen, carbon-dioxide, water vapor or other components in air during sample preparation before measurements. Also, with recent rapid progress in materials science and instrumentation technology, and advances in nano-processing technologies, there is increasing demand to greatly reduce undesirable reactions and contamination. To deal with these issues, the Kyushu Synchrotron Light Research Center has developed and been operating a sample conveyance system with ultra-high vacuum condition (Figure 1) in order to transport samples without exposure to air, such as from a glove box to an analytic chamber equipped with synchrotron beam line facilities. At this time, the Center has collaborated with NICT to develop new technology and advance this system further.

Technology

In this initiative, we have developed a new, portable, a sample conveyance system with ultra-high vacuum condition (Figure 3), combining the earlier sample conveyance system developed and in use by the Kyushu Synchrotron Light Research Center, and a compact, portable, battery-operable UHV pump developed by



Figure 1 Apparatus for moving a sample directly from the glove box to the sample conveyance system



Figure 2 Battery operable compact UHV ion pump It can operate for over 30 minutes on 16 off-the-shelf AA-size batteries.

NICT (Figure 2).

We placed a sample of cobalt metal (Co), which is commonly used as a battery material, in the conveyance system after cleaning under UHV conditions, and then measured any changes in the state of the surface using X-ray photoelectron spectroscopy (Figure 4).

The results of measuring the cobalt surface 2p photoelectron spectrum using X-ray photoelectron spectroscopy is shown in Figure 5.

The shape of the spectrum for the sample stored in the conveyance system (c) is very similar to that of the spectrum immediately



Portable a sample conveyance

system with ultra-high vacuum

condition with compact ion pump

jointly developed by the Kyushu

Synchrotron Light Research

Center and NICT



Figure 4 Measurement equipment at the Kyushu Synchrotron Light Research Center

shows that oxidation of the cobalt surface after cleaning is suppressed to approximately 1/4 of that when left in air.

Using the portable a sample conveyance system with ultrahigh vacuum condition that we have developed, it is also possible to transport delicate and highly reactive samples over long distances to the synchrotron radiation facility for analysis (Figure 6).

Future prospects

This new technology seamlessly connects vacuum environments at users' research locations and the synchrotron radiation facility, enabling highly reliable measurements to be made more easily on samples that are sensi-

tive to air exposure. The technology also enables UHV environments, which are extremely clean, to be created, maintained and transported easily operated by off-the-shelf batteries.

We expect that it can be used for R&D in various fields in the future, such as for collaborative work among multiple research facilities on samples requiring a UHV environment, or when UHV equipment is needed under conditions where a commercial power source is not easily available.

Acknowledgments

This research was conducted in collaboration between the Kyushu Synchrotron Light Research Center, Saga Prefecture, and the NICT Advanced ICT Research Institute. We sincerely thank Dr. Eiichi KOBAYASHI of the Kyushu Synchrotron Light Research Center and all others for their support.



after cleaning (b). This shows that oxidation of the cobalt metal

surface was effectively suppressed while it was stored in the conveyance system. Compared with spectrum (b), the peak intensity

of photoelectrons originating from the cobalt is lower, and the binding energy at the peak is shifted toward high energy (leftward

on the horizontal axis). This indicates that the cobalt metal has absorbed oxygen and other impurities, and a comparison of the

peak areas for the spectrum of photoelectrons emitted by cobalt

atoms and that of photoelectrons emitted by Oxygen atoms (O),

Figure 5 Results of measuring the 2p photoelectron spectrum of a cobalt (Co) surface using x-ray photoelectron spectroscopy

(a) After air exposure, (b) immediately after cleaning, (c) after storing cleaned sample in the conveyance system for approximately 3 minutes.

Figure 6 Sample conveyance concept

Using the compact UHV pump conveyance system, delicate and highly reactive samples can be shared, analyzed and processed among distant research facilities, without damage to basic physical properties.

Report on Exhibit at nano tech 2015



NICT booth

From January 28 to 30, NICT exhibited at the 14th International Nanotechnology Exhibition & Conference (nano tech 2015), held at Tokyo Big Sight.

We introduced our latest research including high-performance electro-optical polymers and high-speed, low-power devices using EO polymers that are contributing to future optical communications, and development of applications using these technologies. Other exhibits included development of practical technologies such as gallium-oxide devices and increasing the efficiency and power of deep-UV LEDs. Companies conducting leading-edge R&D, and also those developing them practically and deploying them in society showed much interest.

nano tech received 47,649 visitors in total over the three days, showing the growth and increasing attention on this field. The NICT booth also received many visitors and visitors exchanged opinions with NICT researchers enthusiastically.

NICT will continue to work, promoting results of our advanced research in nanotechnology and bio-ICT through nanotech trade shows and technical conferences, ensuring that NICT basic technology is developed practically and returned to society, and further strengthening cooperation between academia and industry.



Organic electro-optical polymer exhibit



Advanced device development center exhibit

Report on "Disaster Crisis Management ICT Symposium 2015" and "The 19th Earthquake Technology Expo Yokohama"

On February 5 and 6, 2015, the NICT Applied Electromagnetic Research Institute and the ICT Forum for Security and Safety (President: Dr. Fumio TAKAHATA) exhibited at the 19th Earthquake Technology Expo Yokohama, held at Pacifico Yokohama. Also, on February 6, "Disaster Crisis Management ICT Symposium—Observation and prediction of heavy rain and volcanic eruption damage—" was held in the Annex Hall of the same venue. Two keynote speeches and eight lectures were given at the symposium. NICT speakers included Nobuhiro TAKAHASHI, Director of Radiowave Remote Sensing Laboratory, speaking on "Methods for predicting heavy rain and tornados using radar", Seiho URATSUKA, Managing Director, speaking on "Volcano observations using an airborne SAR system", and Hiroshi KUMAGAI, Associate Director General of the Resilient ICT Research Center, speaking on "Distribution technologies for disaster information". The symposium was attended by approximately 160 people including disaster-prevention staff from local and regional governments, academics, and manufacturers of disaster prevention products.

The Expo featured panel exhibits titled: "Observations of mount ontake using the airborne Polarimetric and Interferometric Synthetic Aperture Radar (Pi-SAR2) system", "Observing localized heavy rain using phased-array weather radar", "Non-destructive inspection of buildings using an infrared two-dimensional lock-in amplifier system", "Non-destructive sensing and testing technology for buildings using electromagnetic waves", and "Earth environmental visualization using Dagik Earth" with exhibits of actual equipment and panel exhibits of disaster countermeasure initiatives from members of the ICT Forum for Security and Safety.

The Expo attracted 15,039 visitors, many of whom visited the NICT booth and showed great interest in NICT's earthquake and disaster countermeasure technologies.



Presentation by Director TAKAHASHI



Lecture by Managing Director



Closing address by NICT Vice President TOMITA



Symposium



NICT booth



Dagik Earth





Phased-array weather radar exhibit

Report on Exhibit at SECCON CTF 2014 Finals

-NIRVANA Kai SECCON Custom Mk-II excels at capture the flag cyber battle-

The NIRVANA Kai SECCON Custom Mk-II, developed by NICT Cybersecurity Research Center (CYREC) was exhibited at the security contest: SECCON CTF 2014 Finals, held at Tokyo Denki University on February 7 and 8, 2014. SECCON CTF is the largest Capture The Flag (CTF) cyber security competition in Japan, held in order to nurture excellent information security technologists, raise their skill level, and protect enterprises and organizations from recently intensified cyber attacks and malware infections. The best team from this year's competition wins the right to compete at DEF CON® CTF, held in Las Vegas. DEF CON CTF is the pinnacle of CTF competition so at this competition, the top CTF teams were gathered from around the world.

In SECCON CTF, teams compete on the total of both attack points and defense points. Here, "attack" refers to solving a given problem. At SECCON CTF, various problems on security themes, such as Web server attacks or cryptanalysis, were prepared on a problem server. When these problems are "captured" the team is awarded attack points. Conversely, defense points are gained for occupying a problem server. Such problem servers can be occupied by writing a keyword at a specified location on the server. Defense points are divided among occupying teams, resulting in more points awarded

if there are fewer occupying teams, so occupying teams must defend the server against occupation by other teams.

Exhibited at this meet was NIRVANA Kai SECCON Custom Mk-II, a version of the NIRVANA Kai, integrated analysis platform engine, which supports targeted attacks and other high-level cyber attacks. This version was developed to visualize CTF events and with other enhanced functionality compared to early versions. For this competition, problem servers were shown as blue hexagonal towers, and teams were shown as orange hexagonal towers. Attacks on problem servers appeared as orange energy waves, and occupation of a server as a yellow flag. In addition to showing capture of problems and occupation of servers, communication resulting from attacks and defense is also visualized, so the tactics of each team can be seen at a glance.

Many CTF players are active in the security industry, and CTF plays an important role in nurturing and expanding the base of security personnel and improving their skills. NICT will continue cooperation with SECCON CTF in the future, using research results in CTF, and contributing to the education of security personnel.



NIRVANA Kai SECCON Custom Mk-II (Tower mode)



NIRVANA Kai SECCON Custom Mk-II (Plane mode)

Report on 100 G Multicast Test and International Transmission to Thailand Test on JGN-X

On February 6, 2015, the NICT Network Testbed Research and Development Promotion Center conducted a demonstration at Knowledge Capital, the Grand Front Osaka using the JGN-X network testbed. The test used the JGN-X 100 Gbps core circuit, upgraded in 2014, to transmit multiple 8K uncompressed multicast streams between the NICT Network Testbed Research and Development Promotion Center in Tokyo, Knowledge Capital in Osaka, and NICT Hokuriku StarBED Technology Center in Hokuriku. It was the first successful test of its kind in the world. Scenery from Sapporo and Otaru was displayed on 8K displays at the Osaka venue, and many visitors were able to see the high-definition video and exhibits of the latest technology used to achieve the transmission.

On the same day, real-time 60 fps 4K video of the Snow Festival was transmitted using the JGN-X international line from Sapporo to the "Next-generation TV and Ultra-high-speed Network Seminar" in Bangkok, Thailand. The Seminar was organized by the Ministry of Internal Affairs and Communications and Thai-related agencies such as the Japanese Embassy in Thailand and NECTEC were invited. Japan's high-definition video technologies were also promoted at the event, with an exhibit of 4K high-definition video from NICT and booths from Japanese manufacturers developing 4K televisions.





Demonstration at Grand Front Osaka

8K display (prototype from Sharp Corp.)



Measurements of the connection for uncompressed 8K transmission at Osaka



4K relay via JGN-X from Odori Park in Sapporo City to the venue in Thailand



Opening greeting from NICT Vice President, Makoto IMASE at the seminar in Bangkok, Thailand



Exhibit of 4K ultra-high-definition image at the seminar

Popular on Twitter! --NICT familiarity increasing-

NICT is providing its latest information to the public through various media.

@NICT_Publicity

One such medium is Twitter, which provides easy access to the latest information using mobile phones and tablets, and has become quite popular recently. NICT is publishing the latest NICT information, including press release and event information, through our official Twitter account. Please follow us!

https://twitter.com/NICT_Publicity



Notice of Organization Status Change

As of April 1, 2015, NICT will change from being an "**Incorporated Administrative Agency**" to being a "**National Research and Development Agency**" according to revisions to the Act on General Rules for Incorporated Administrative Agencies.



Published by Public Relations Department, National Institute of Information and Communications Technology <NICT NEWS URL> http://www.nict.go.jp/en/data/nict-news/ ISSN 2187-4034 (Print) ISSN 2187-4050 (Online)

> 4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan Tel: +81-42-327-5392 Fax: +81-42-327-7587 E-mail: publicity@nict.go.jp <NICT URL> http://www.nict.go.jp/en/