NTU GICE Newsletter
Graduate Institute of Communication Engineering, National Taiwan University
Vol. 10, No.1 Feb. 2019 https://comm.ntu.edu.tw/ gicenewsletter@ntu.edu.tw

In this issue

Technology Developed in GICE

Privacy Preserving Machine Learning

from Data Science and Smart Networking Group

INTRODUCTION

In an era where distributed computing and storage systems have grown vigorously, much of the data are being collected among various data owners and analyzed by machine learning (ML) algorithms. To venture ML services into more sensitive (and often more impactful) applications, the issue of privacy preserving against abusive usage of those sensitive personal data, such as medical records and personal opinions, becomes an important issue.

The main stream of privacy preserving ML includes randomized-based method such as differential privacy (DP) and local differential privacy, the cryptographic-based methods such as homomorphic encryption (HE), as well as information-theoretic (IT) privacy. In the randomized-based method, noise is added in the data and/or the learning algorithm, making it difficult to infer one specific data entry from the released model (and hence preserves privacy). The extent to which privacy is preserved is well-quantified by the privacy budget in the DP/local DP literature. However, randomized-based method may still leak the general statistics of the data set provided by an individual data owner. Furthermore, adding noise may lead to degradation of the model accuracy performance.

In homomorphic encryption (HE), based on the special property that an addition on the plain text is homomorphic to a well-defined operation (e.g., modular multiplication) on the cipher text,

(Continued on page 2)

GICE Honors

Prof. Chun-Ting Chou
「2019 CES Innovation Award」

Prof. Tzong-Lin Wu
「IEEE T-CPMT Best Associate Editor Award」

Message from the Director

Hsuan-Jung Su

Professor & GICE Director

Happy Chinese new year, everybody! In the new year, we are pleased to share the great news of our professors' research and technology achievements. The OmniEyes startup team led by Prof. Chun-Ting Chou won the CES 2019 innovations award, and Prof. Tzong-Lin Wu won the "IEEE T-CPMT Best Associate Editor Award". Big congratulations to our professors for international recognition!!

In this issue, we invite Prof. Pei-Yuan Wu to share his research results on preserving privacy for the data analyzed by machine learning algorithms, which is a very important issue in the era of big data. Prof. Shih-Yuan Chen also shares his research results on microwave holographic imaging. In the Corner of Student News, we are happy to have Siddhartha Panigrahi, a Ph.D. student at NTU GICE, share his personal experience living in Taiwan. Please enjoy reading this issue and I wish you wonderful Chinese new year holidays.

Technology *(Continued from page 1)*

the data owner can encrypt their raw personal data before sending to the data user, who performs arithmetic operations on the cipher text to realize ML algorithms without knowing the sensitive plain text in the first place. Despite its safety, HE is often criticized for its costly computation on data encryption/decryption. Moreover, it is often required in multi-party computation that all the parties should stay online, leading to scalability issues.

In IT privacy, privatization mechanism is applied to the raw personal data before releasing to the cloud, so that the private sensitive information leakage is minimized under a fixed budget of tolerable data distortion. However, the joint probability distribution of the sensitive data and the released data is required in designing the privatization mechanism, which is often impractical to acquire.

Thanks to the tremendous success of the deep neural networks, especially the development of the generative adversarial network (GAN), data-driven IT privacy are proposed where the privatization mechanism is realized by the generator network, whose goal is to fool the adversary who aims to infer sensitive information from the released data through an adversarial network. In the following, we will discuss how the GAN-inspired privatizer is designed, as well as several results in image recognition applications.

Data Driven Privatization Mechanism

Consider the scenario where Alice holds personal raw image data x and wishes to enjoy the image recognition service provided by Bob on the cloud, which predicts the category y of the image. If Alice sends the raw image directly to the cloud, it will suffer the risk of falling into the wrong hands of malicious adversary Eve. To preserve privacy, Alice instead applies a privatization mechanism G to nonlinearly transform x into privatized data z=G(x), and releases z to Bob through the cloud. There are two purposes: (1) From the utility perspective, the privatized data z should have sufficient information for Bob to provide image classification service; (2) From the privacy perspective, it should be difficult for Eve to reconstruct x from the privatized data z.

Motivated by the adversarial training idea from GAN, the privatization mechanism (G) from Alice, the utility classifier (C) from Bob, and the reconstructor (R) from Eve can all be realized as deep neural networks as illustrated in Figure.1. Here we consider the following loss function

$$\max_{G}\left(\min_{R}\mathbb{E}_{\substack{(x,y)\sim P_{data}\\ \varepsilon\sim P_{noise}}}[\|\boldsymbol{x}-\hat{\boldsymbol{x}}\|^2]+\lambda\max_{R}\mathbb{E}_{\substack{(x,y)\sim P_{data}\\ \varepsilon\sim P_{noise}}}\left[\sum_{i=1}^{L}y_i\log\hat{y}_i\right]\right) \#(1)$$

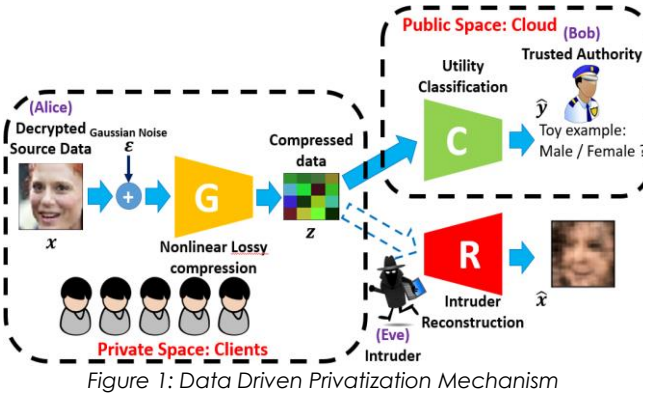

Figure 1: Data Driven Privatization Mechanism

(Continued on page 3)

Technology *(Continued from page 2)*

More elaborately, the adversary trains the reconstructor network aiming to achieve the best reconstruction by minimizing the mean squared error (MSE) between reconstructed image $\hat{x}=R(z)$ and the raw image x, while the utility network aims to achieve the highest classification accuracy to provide better service. The goal is to design the privatization network so that even the best reconstructor network can hardly reconstruct the raw image, while at the same time the utility network's performance can be maximized.

Result

The data driven privatization mechanism is tested on CIFAR-10 and SVHN data sets. To illustrate the privacy aspect, we illustrate the original image and the reconstructed images by the adversary in Figure 2 (CIFAR-10) and Figure 3 (SVHN). To illustrate the utility aspect, we list the utility classification accuracy for both data sets in Table 1. Note that in the related previous work [1][2], the classification is based on the raw image x, which suffers the risk of falling into the wrong hands where the adversary gets access to the raw image (1st row in both Figure 2 and Figure 3). On the contrary, with privatization mechanism, only the privatized data z is released to the cloud, from which the adversary is difficult to reconstruct the raw image in a recognizable way (2nd row in Figure 2 and Figure 3). The enhancement in privacy is achieved at a cost of utility accuracy degradation (96.45% to 93.87% in CIFAR-10, and 98.6% to 97.7% in SVHN).

Figure 2: CIFAR-10 Adversarial reconstruction

Figure 3: SVHN Adversarial reconstruction

Method	Released Data	CIFAR-10	SVHN
Privatization	Compressed	93.87%	97.7%
Gastaldi [1]	Original	96.45%	98.6%
Zagoruyko [2]	Original	92.83%	98.3%

Table 1: Utility accuracy comparison

Conclusion

In this research a data driven privatization mechanism is implemented based on the adversarial training formulation idea behind GAN. Experimental results show that (1) the privatized data achieves satisfactory utility performance, while (2) it is difficult for the adversary to reconstruct the original data in a recognizable way based on the released privatized data, hence preserving privacy. This research verifies such data-driven privatization mechanism can be implemented on image recognition applications, which can be further extended to other applications such as acoustic, biometric, or medical data as future work.

Reference

[1] X. Gastaldi, "Shake-shake regularization of 3-branch residual networks", in International Conference on Learning Representations Workshop Track, 2017.
[2] S. Zagoruyko and N. Komodakis, "Wide Residual Networks", in BMVC 2016.

For more information please contact:
Professor: Pei-Yuan Wu
Email: peiyuanwu@ntu.edu.tw

Technology

Three-Dimensional Microwave Holographic Imaging with Probe and Phase Compensations

from Electromagnetics Group

Microwave imaging is a process of solving inverse scattering problem, which is able to retrieve the properties of unknown targets by measuring and analyzing the field scattered by the targets. Owing to the penetrating and non-ionizing characteristics, microwave imaging has found wide applications [1], [2]. Following the trend, various microwave holographic imaging algorithms have been developed, including those from 2-D to 3-D, from far-field to near-field, and from scalar-wave-based to vector-wave-based imaging. Most of the previous algorithms did not take into account the receiving characteristic of the probe antenna and only assumed that the receiving response of the probe antenna is proportional to the scattered field at the phase center of the probe antenna. The assumption holds true if a short dipole is adopted. However, in practice, antenna with a higher gain, such as a horn antenna, is used to obtain a stronger scattering response, and hence a higher signal-to-noise ratio (SNR). As a result, the assumption is inappropriate. To tackle this, we proposed a 3-D microwave holographic imaging algorithm compatible with single-probe reflection-coefficient measurement [3]. The imaging model is depicted in Fig. 1. The proposed holographic imaging algorithm can be divided into four parts. First, starting from the open-circuit voltage of antenna, the algorithm compensates for both transmitting and receiving properties of the probe antenna, leading to antenna-independent least squares problems. Generally, the problems tend to be ill-conditioned, thus, an auxiliary equation is derived and exploited to effectively improve the numerical stability and image quality. Third, to accurately locate the unknown target in range direction, a novel phase compensation method that requires only phase correction to the associated entries of the kernel matrix is proposed based on a simple ray model. Last, considering the finite size of the scanning aperture and beamwidth of the probe antenna, a numerical low-pass filter in the spatial-frequency domain is utilized to effectively sieve out the worth-solving area.

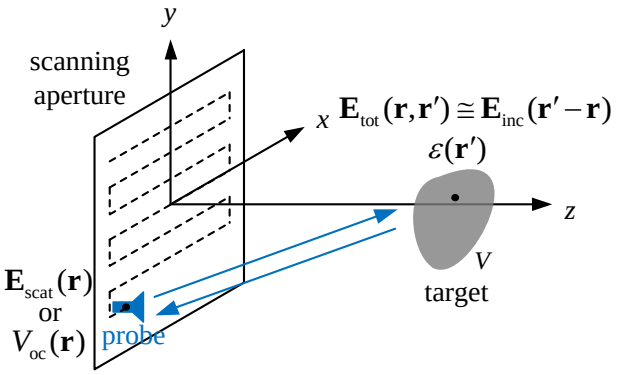

Fig. 1. Planar scanning setup for the proposed imaging method.

To demonstrate the efficacy of our proposed method, a series of images are reconstructed from the simulated data using the proposed algorithm. Simulations are first performed using FEKO, and then the simulated scattering data are used to reconstruct the images on the predetermined observation z-planes. Figs 2(a) and (b) illustrate the simulation setups for two types of probe antennas, i.e., a half-wavelength dipole and a microstrip patch antenna, which show the flexibility of the proposed algorithm in choosing probe antenna. The reconstructed slice images on the three chosen observation planes, namely z 57, 60, and 63 mm, are shown in Figs. 3(a) and (b), respectively. Obviously, the images retrieved via the two setups resemble each other, and the target indeed appears in the slice image at the z 60 mm observation plane. Importantly, the proposed algorithm can accurately estimate the dielectric constant of the target in both cases.

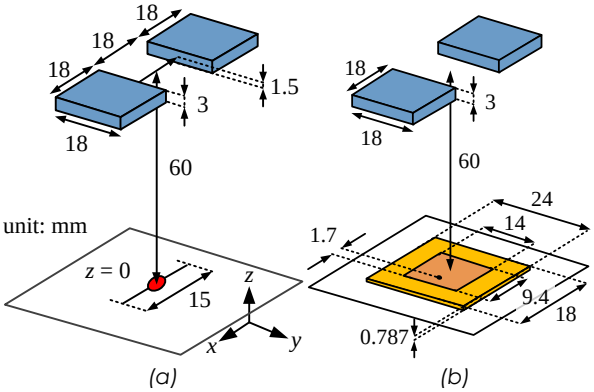

Fig. 2. Scanning setups for a pair of dielectric cuboids as target using (a) a half-wavelength dipole and (b) a patch antenna, respectively.

(Continued on page 5)

Technology *(Continued from page 4)*

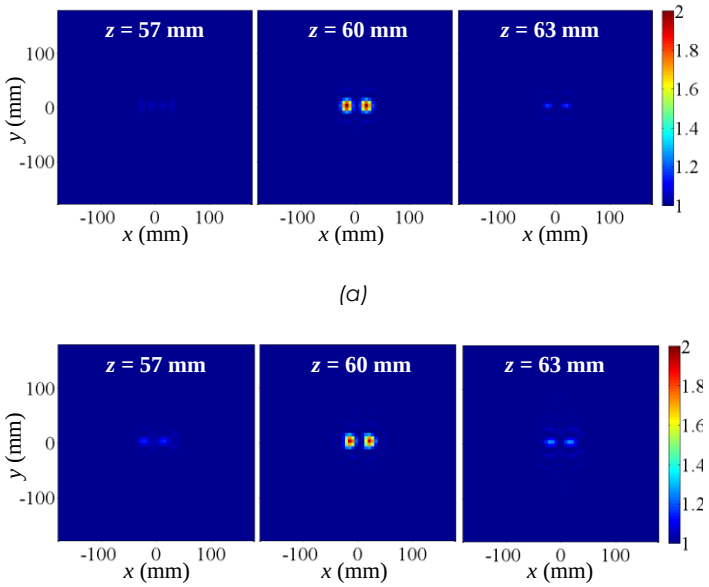

Fig. 3. Reconstructed images using the proposed algorithm and (a) a half-wavelength dipole and (b) a patch antenna as the probe antenna, respectively. Both antennas are designed at 10 GHz.

To further exhibit the effectiveness of the proposed algorithm, a single-antenna reflection-coefficient measurement system was used. A photograph of the setup is depicted in Fig. 4. It consists of a laptop computer, a vector network analyzer (VNA), a three-axis motorized scanner, which is formed by a three-axis motorized stage and a stage controller, and a horn antenna that can operate from 8.2 GHz up to 12.4 GHz with an average gain of 10 dBi. The reconstructed images of the practical targets using the proposed algorithm are illustrated in Fig. 5. Although some minor artifacts can be observed, the shape and dielectric constant of the target can still be retrieved with high accuracy. In conclusion, the proposed algorithm not only facilitates and guarantees the reconstructed image quality but also achieves cross-range resolutions of about /4 and range resolution of approximately /10, which is detailed in [3] both quantitatively and qualitatively.

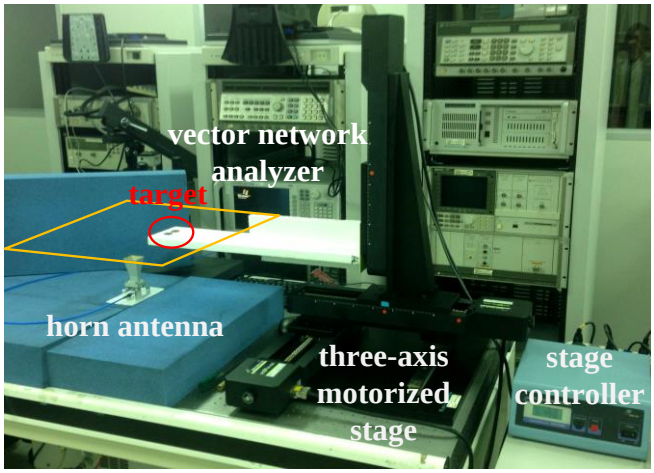

Fig. 4. A photograph of the experimental scanning setup.

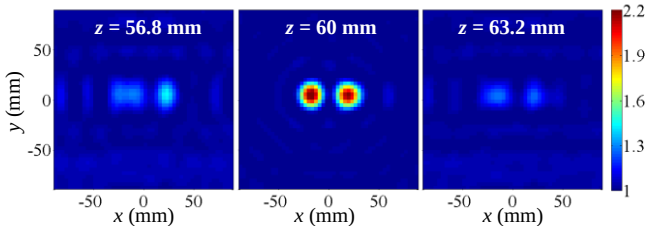

Fig. 5. Images reconstructed by the proposed algorithm and based on the scattering data measured via the setup of Fig. 4.

References

[1] L. Carin, J. Sichina, and J. F. Harvey, "Microwave underground propagation and detection," IEEE Trans. Microw. Theory Tech., vol. 50, no. 3, pp. 945-952, Mar. 2002.

[2] D. M. Sheen, D. L. McMakin, and T. E. Hall, "Three-dimensional millimeter-wave imaging for concealed weapon detection," IEEE Trans. Microw. Theory Tech., vol. 49, no. 9, pp. 1581-1592, Sep. 2001.

[3] C.-H. Tsai, J. Chang, L.-Y. Ou Yang, and S.-Y. Chen, "3-D Microwave Holographic Imaging With Probe and Phase Compensations," IEEE Trans. Antennas Propag., vol. 66, no. 1, pp. 368-380, Jan. 2018.

For more information please contact:
Professor: Shih-Yuan Chen
Email: shihyuan @ntu.edu.tw

Activities

OmniEyes from NTU won the CES 2019 Innovation Award

Under the support of Ministry of Science and Technology's Startup program, the OmniEyes startup team led by National Taiwan University's professors (Professor Chun-Ting Chou, Professor Ai-Chun Pang, Professor Shou-De Lin, and Professor Hung-Yi Lee) created a solution in which can collect and digitize live street videos, and converts them using AI technologies to location-based information. These information can then be used to offer brand new applications to create brand new smart city solutions.

OmniEyes' solution has been recognized internationally, and has been award the CES 2019 innovations award. As the world's gathering place for all those who thrive on the business of consumer technologies, the CES's innovations award is evidence of OmniEyes' potential.

OmniEyes collects and digitizes live street videos, and converts them using AI technologies to location-based information. Our lightweight fog AI along with cloud machine learning engines for interconnected mobile cameras is applicable to many verticals including digital map, fleet and logistics management, mobile advertisement, navigation and advanced driver assistance systems (ADAS), etc. The platform is already in the pilot stage with Taipei City and several commercial fleets and deployed for several

(Continued on page 7)

Activities

(Continued from page 6)

applications. OmniEyes will expand to North America and Southwestern Asia market, and create new markets in the areas of visual guidance, fleet management, intelligent courier service, and dynamic map service and autopilot navigation. OmniEyes team is successful in fund raising and has started a startup company to promote the solution.

Looking back five years when communication market is still focused on cloud computing, Professor Chun-Ting Chou, Professor Ai-Chun Pang has already started exploring the possibilities of fog AI. With great enthusiasm and devotion, the two professors and great effort from the team, Omnieyes team is able to come up with a tangible solution of which won the support of Ministry of Science and Technology's Startup program, formed a competitive team of which is able to commercialize the solution and promote it to the global market.

Special thanks to the Ministry of Science and Technology, Taiwan Startup Institute, National Taiwan University, Industry Liaison Office of National Taiwan University, Taipei City Government, Industrial Technology Research Institute, Chunghwa Telecom Co., Ltd, and Kingway Technology. Special thanks also goes to the consulting team of the project - Dr. Jason Yi-Bing Lin, Dr. Russell Hsing and Dr. Zhang Tao.

Photo with Minister of MoST- Liang-Gee Chen

Group Photo of OmniEyes Team

Corner of Student News

Siddhartha Panigrahi came from India; he got his Master Degree at NTUGICE and he is pursuing Ph.D Degree at NTUGICE now.

National Taiwan University is one of the most prestigious universities in the world for EE and right away was on my preference list for higher studies. However, I had zero knowledge about Taiwan before I landed here. All I knew was this is a small island somewhere in the Pacific boasting a myriad of landscape ranging from mountains to sea beaches. Amazing reviews about the hospitality and friendliness of the people (thanks to Google!) swayed me to pursue my Masters here.

I had a bit of culture-shock. This country is entirely different from my home land. Food, people, language, teaching style --- literally everything! I am a big fan of spicy food with zero Chinese speaking ability and chopsticks are something I had seen only on TV —none of which helps if you really want to be a part of Taiwan. I was very skeptical about my survival but was determined to give my decision a try!

Thanks to my guide and lab mates, I was slowly introduced to the better side of this country. Although the food seemed plain, it was quite delicious and very healthy. Taiwanese people are, in general, warm and accepting. Mostly shy and humble, but very kind. I don't speak Chinese at all, but can go on solo trips across Taiwan because people are willing to help a non-Chinese speaking foreigner. Taipei is one of the safest places with minimum crime rates. You can literally walk/ride at any time of the day/night without any concern for safety. It is amazing how Taiwan has maintained a balance between modernization and tradition. The picturesque landscapes and the versatile scenery of Taiwan make it one of the must-visit exotic places for any travel lover like me!

As said before, NTU is one of the leading universities in EE in the world. The teaching here is more research based. As a Master student, I handled my project individually which gave me the chance to learn a lot. Being independent facilitated all-round understanding of my project and made me more confident in my research. My satisfaction with my Masters can only be explained by my decision to pursue my PhD here without having a second thought!

All in all, Taiwan is a fresh experience for people who need a balanced life. You can shuffle between a posh city life and an exotic country life any time with minimum travel. Coming to Taiwan has shown me a different side of the world and myself. I am in love with this country and plan to stay a few more years here to explore this beauty called Taiwan!

National Taiwan University
Graduate Institute of
Communication Engineering

No.1, Sec.4, Roosevelt Road,
Taipei 10617, Taiwan

Phone
+886-2-3366-3075

Fax
+886-2-2368-3824

E-mail
gicenewsletter@ntu.edu.tw

Visit us at:
http://www.comm.ntu.edu.tw

Editor in Chief
Prof. Borching Su

Editor
Chiao Yun Kang