NTU GICE
Newsletter
Graduate Institute of Communication Engineering, National Taiwan University
Vol.17 No.2 June, 2025 https://gice.ntu.edu.tw/ ntugice@ntu.edu.tw

GICE Honors

NTUEE- 1975 Alumni Award for Technological Research and Innovation – Special Award.

Prof. Hsi-Tseng Chou's research team

The team developed a low-cost and high-efficiency 5G FR2 antenna technology, which won 7th place (out of 119 teams) in the global TIE Award competition organized by the Ministry of Science and Technology in 2022. In 2023, the technology attracted investments from five listed companies and led to the founding of swart Inc.

NTUEE - 1975 Alumni Award for Technological Research and Innovation.

Prof. Yu-Chiang Frank Wang's research team

The team's research was accepted by the 2025 International Solid-State Circuits Conference (ISSCC) and selected as a conference highlight paper. The study presents the first chip in literature to fully utilize video information and characteristics for video super-resolution. Through optimized design, the chip achieves superior frame rate and energy efficiency compared to existing systems. It has potential applications in high-speed, high-efficiency, and high-resolution mobile devices.

Metamaterial-Enhanced Radar Sensors for Multi-Target Vital Sign Monitoring and Location Tracking

Dr. Chung-Tse Michael Wu

Associate Professor
Graduate Institute of Communication Engineering
National Taiwan University

Radar technology has gained significant traction as a contactless, noninvasive solution for monitoring human health—particularly in vital sign detection applications for elderly care, home-based healthcare, and even through-wall sensing. Unlike traditional physiological monitoring devices such as electrocardiograms (ECGs) or finger pulse oximeters, radar sensors utilize electromagnetic (EM) waves to detect subtle physiological motions remotely. This contactless approach not only improves user comfort and compliance but also enables continuous, real-time monitoring without physical constraints.

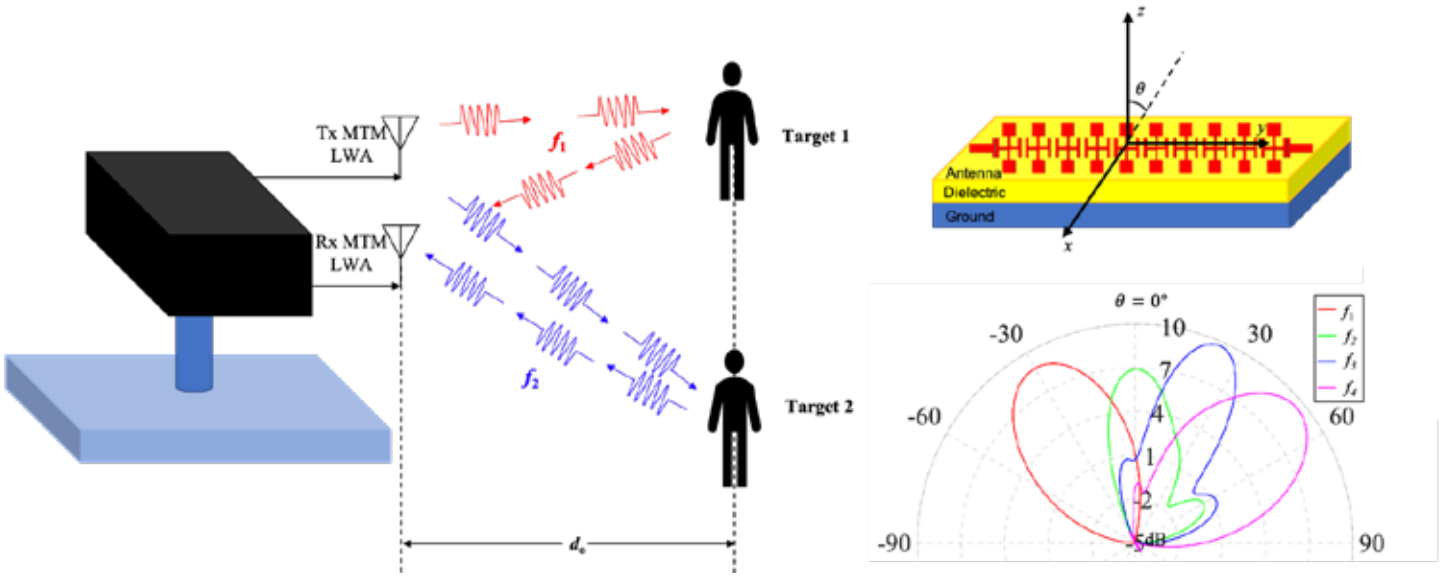
Among the various radar architectures developed for physiological monitoring, the homodyne transceiver is one of the most widely used. In a conventional homodyne radar system, a transmitting antenna (Tx) emits a continuous-wave radiofrequency (RF) signal toward a human target. As the RF signal reflects off the body, it becomes modulated by minute physiological movements—primarily chest displacement due to respiration and heartbeat. This reflected signal is captured by a receiving antenna (Rx), and subsequently down-converted into baseband in-phase (I) and quadrature (Q) signals using an RF mixer. The Doppler frequency shift caused by target motion provides critical information about the subject's distance and vital signs.

While this technique has been proven effective for single-subject monitoring, conventional homodyne systems face significant limitations when scaled to multi-target scenarios. Detecting multiple individuals typically requires more complex hardware or scanning techniques, such as mechanical beam steering, phased array antennas, or digital beamforming. These enhancements, although functional, often increase system cost, size, and complexity, making them less practical for compact, cost-sensitive healthcare or consumer applications.

To address these limitations, researchers have turned to metamaterials (MTMs)—engineered artificial structures with unique electromagnetic properties not found in naturally occurring materials. First proposed by Viktor Veselago in 1967, metamaterials exhibit extraordinary phenomena such as negative refractive index, which can be exploited to manipulate wave propagation in novel ways. In practical implementations, transmission-line (TL) approaches have been used to realize MTM structures capable of supporting leaky-wave propagation. In particular, metamaterial leaky-wave antennas (LWAs) operating in the fast-wave regime can steer their radiation beam across a wide angular range simply by changing the operating frequency. This frequency-dependent beam scanning enables the radar to interrogate multiple spatial locations without requiring any physical movement or active beamforming circuitry.

Our research group has leveraged this property to develop several compact radar systems using MTM LWAs at millimeter-wave frequencies, such as the 24 GHz band. These systems are capable of detecting vital signs and tracking motion for multiple spatially separated targets. Unlike traditional systems, no mechanical scanning or complex digital beamforming is required—resulting in dramatically reduced system cost, footprint, and power consumption. This compact and efficient approach opens new possibilities for real-time, multi-person monitoring in smart homes, clinics, and public spaces.

To further enhance sensitivity and simplify radar system architecture, we introduced a novel design that integrates the MTM LWA with a superregenerative oscillator (SRO). The SRO is a century-old concept that has recently been revitalized due to advancements in nonlinear dynamics and circuit design. It operates by periodically quenching an oscillator between stable and unstable states using an external modulation signal. During each active cycle, the oscillator exponentially amplifies weak input signals through positive feedback, while noise is suppressed during the quiescent intervals. This time-varying amplification mechanism not only provides exceptional sensitivity but also reduces power consumption—making it ideal for low-power sensing and communication systems.



In our configuration, the SRO generates the RF signal that is transmitted via the MTM LWA. When this signal reflects off a human target, the returning wave—modulated by cardiopulmonary activity—is coupled back into the oscillator circuit. The reflected signal perturbs the oscillator's internal dynamics, causing changes in the oscillation envelope. This interaction effectively embeds the target's physiological information into the oscillator's output. Because the SRO's behavior is inherently nonlinear and highly sensitive to weak signal variations, it serves as both a signal generator and a demodulator in a single compact component.

The output of the SRO contains amplitude variations corresponding to respiratory and cardiac motion. These baseband envelope signals can be extracted using simple signal processing methods such as envelope detection, low-pass filtering, and fast Fourier transform (FFT). Unlike conventional radar systems, there is no need for RF mixers, intermediate frequency (IF) stages, or complex I/Q demodulation chains. The result is a minimalist radar architecture with reduced hardware requirements, enhanced energy efficiency, and simplified signal processing.

Moreover, the SRO's inherent frequency selectivity further eliminates the need for external RF filters, streamlining the overall system design. Its capability for high gain and narrowband detection makes it especially effective for applications involving weak signals. These advantages have led to its growing use not only in vital sign monitoring but also in low-power wireless communication, millimeter-wave imaging, and Internet of Things (IoT) applications.

By combining the frequency-scanning functionality of MTM LWAs with the sensitive, low-complexity nature of SROs, we have developed a new class of radar sensors capable of concurrent multi-target tracking and real-time vital sign monitoring. This integrated approach addresses the major challenges faced by traditional radar architectures—eliminating bulky scanning hardware and expensive beamforming arrays, while enhancing system robustness and scalability.

In conclusion, metamaterial-enhanced radar sensors utilizing superregenerative oscillators represent a promising direction for the next generation of biomedical sensing systems. These platforms are compact, energy-efficient, and capable of supporting real-time, contactless monitoring for multiple individuals. Their unique combination of advanced electromagnetic design and nonlinear circuit dynamics paves the way for a wide range of applications, from in-home health monitoring to wearable devices and smart infrastructure. As healthcare continues to move toward personalized, remote, and unobtrusive solutions, the role of such advanced radar systems is poised to grow significantly.

Two Applications of Shannon Entropy, the Second One Might Be Surprising

Dr. Hsin-Po Wang

Assistant Professor
Graduate Institute of Communication Engineering
National Taiwan University

The mathematical core of modern communication systems is the information theory initialized by Shannon in 1940s. At the core of this theory is the entropy function, called Shannon entropy, that measures the amount of information we know or we don't know. The theory tells us that, in a communication system, the receiver can never receive more information than what the sender sent, minus some information loss due to noise. But that's just an theoretical bound. In reality, engineers still need to figure out implementation details so that the theoretical bound is met. Therefore, the more we know about the Shannon entropy, the better we can design communication systems.

But Shannon's theory does not stop there. Let's take a look at two more applications of Shannon entropy that are beyond the scope of communication systems.

Random number generation

Generating random numbers is a common task needed in every corner of STEM fields. In cryptography, one needs to generate random keys that cannot be predicted by the big brother. A textbook example of what not to do is to generate a password by asking the user to think of a random four-digit number, abcd, and repeat this number three times: abcdabcdabcd. Now, I cannot claim that this provides twelve digits of security, because every attacker with a sane mind only needs to try 10,000 combinations. What is worse, the attacker can even guess that abcd is very likely 1234, 5566, or 2025, and so it can break the password in probably 1000 tries.

In physical simulations and machine learning, the same problem exists. We need a large amount of high-quality random numbers that are not just abcdabcd. Usually we are taught to use syntaxes like `rand() % 100` to get a random number between 0 and 99, but there is a problem.

In C, for instance, the `rand()` function returns a pseudo-random number between 0 and `RAND_MAX`, which is at least 32767 by the C standard. While using 32767 makes the function fast, it's too small, even smaller than the number of seconds in a day. What is worse, the distribution of the last digit is not uniform in some implementations. If you use `rand() % 2` to simulate the stock price of a single stock for a day, where the price can go up or down every second, you will call `rand()` 86400 times and it might, depending on the version of your C compiler, repeat itself. In a way, this is not too different from the abcdabcd example above, just that the repetition is not obvious and harder to detect, making it even more dangerous.

From the discussion above, we see that the best practice is to get a high-quality entropy source, something similar to a Geiger counter, and build a protocol that can convert the source into a random number. We have to keep in mind that a high-quality entropy source takes a lot of time to collect data. We also have to keep in mind that the entropy of the protocol's output is never larger than the entropy of the source. So, in particular, we should not use `Geiger_count() % 2` because all but the last bit is wasted. Instead, we can use `G % 2` for day one, `(G / 2) % 2` for day two, `(G / 4) % 2` for day three, and so on, where `G` is the output of the Geiger counter. Through this, we can simulate the stock price for a longer period of time per use of the Geiger counter.

Now, there is a tiny problem with this approach. Suppose that we want to simulate the stock price of a company with a bright future, and so we want the price to go up 70% of the time. This means that, out of the same Geiger counter output `G`, we want to extract Bernoulli random variables with mean 0.7. An obvious solution is to use `(G % 10) < 7` for day one, `((G / 10) % 10) < 7` for day two, and so on. But let's check this protocol with Shannon entropy: Suppose that `G % 10` is uniformly distributed in {0, 1, ..., 9}, the entropy of `G % 10` is log2(10) bits, or about 3.32 bits. The entropy of the Bernoulli random variable is -0.7 * log2(0.7) - 0.3 * log2(0.3) bits, or about 0.88 bits, which is a quarter of the former.

That is to say, we could have simulate the stock price for four times as long per use of the Geiger counter, if we manage to find a better protocol. Furthermore, after we find such a protocol, we should go back to modifying the Geiger counter and make sure that `G`, `G % 2`, `G / 10`, etc. are uniformly distributed.

This problem is known for decades and many big names have worked on this, including Knuth, Yao, von Neumann, Elias, and Han. It has deep connections to data compression, including the famous arithmetic coding, interval coding, asymmetric numeral systems, and combinatorial number system. After all, converting the output of a Geiger counter to uniform Bernoulli is like compressing `G` into a binary string; generating a biased Bernoulli is like decompressing the binary string as if the string is a compressed file. What remains an open problem is to find a protocol that can do both at once: Converting a biased `G` to arbitrary discrete distributions. Finding better protocols help us do Monte Carlo simulations and stochastic optimization more efficiently and with better theoretical guarantees.

Query complexity

Modern databases often come with powerful algorithms that can answer creative questions from users. For instance, Squid Game is a very successful TV series, and its producers want to know what to do next. They can ask the database to find out, among the audiences who give Squid Game thumbs up, what else do they like? What movies and TV series do they watch? For how much screen time? Are there people that watch the same genre of movies and TV series that could be potential audiences? The answers to these questions can help the producers make better decisions on the next season.

To answer these questions, databases systems often come with efficient algorithms and can go over the entire dataset in no time and, say, return a list of audiences that match the criteria. One essential aspect of optimizing algorithms is to make the most out of the memory hierarchy. For instance, L3 cache is 10x faster than RAM, RAM is 10x faster than SSD, and SSD is 10x faster than HDD. (This is just a rule of thumb, the actual numbers vary from brand to brand.) So caching data in L3 can significantly speed up access times, which is often the dominant factor in query complexity. If the data do not fit in L3 cache, caching in RAM is the next best thing, and so on.

But there is a problem, it is hard to predict the size of the intermediate data in advance. For instance, the producer might want a list of audiences that like one movie and one TV series that a Squid Game liker also likes.

That is, we want to find all tuples (a, m, t, p), where a is an audience that likes Squid Game, m is a movie that a also likes, t is a TV series that a also likes, and p is the potential audience that likes both m and t. Without knowing how many tuples are there, it is hard to predict how much memory they need. This is where Shannon entropy comes in. Imagine that we have the list of (a, m, t, p)-tuples, and we draw a random tuple (A, M, T, P) from the list. Then the entropy of this random tuple is H(A, M, T, P) = log2(the length of the list).
Thus, having an estimate of the entropy is equivalent to having an estimate of the size of the list; this determines the level of cache we can afford, as well as how many CPUs and threads are needed to process the list.

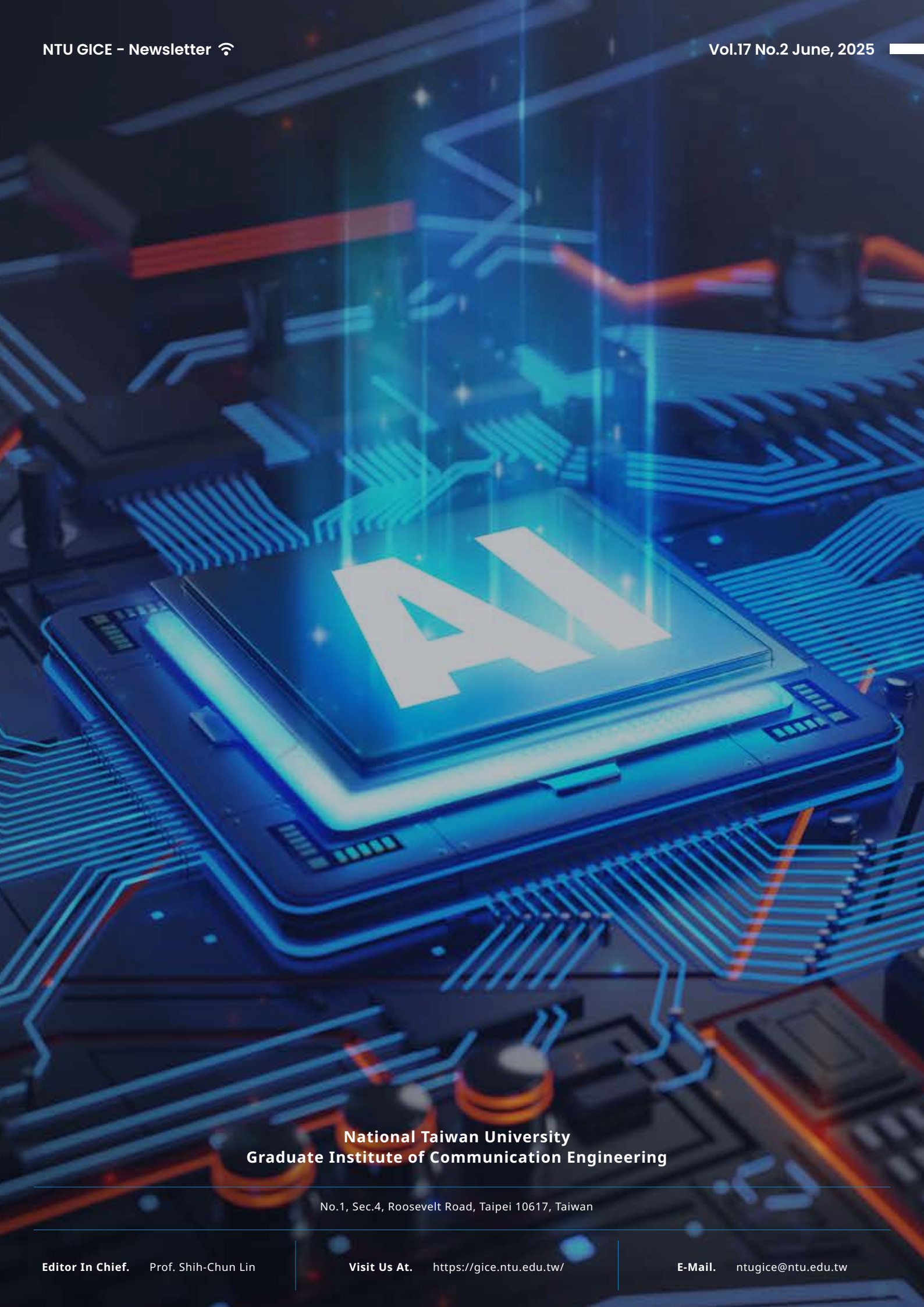
Now Shannon entropy comes with a series of inequalities, called the Shannon-type inequalities. For instance $H(A, M, T, P) \leq H(A) + H(M) + H(T) + H(P)$; this suggests that the length of the list is at most two to the power of H(A) + H(M) + H(T) + H(P). This is equivalent to saying that the number of (a, m, t, p)-tuples is at most the number of audiences squared times the number of movies times the number of TV series, which is not very useful. But Shannon can do better. For instance, $H(A, M, T, P) \leq H(A, M) + H(T, P)$, meaning that the number of (a, m, t, p)-tuples is at most the number of (a, m)-tuples times the number of (t, p)-tuples.

We can also form inequalities with conditional entropies, such as $H(A, M, T, P) \leq H(A, M, T) + H(P \mid M)$ and $H(A, M, T, P) \leq H(A, M) + H(T \mid A) + H(P \mid T)$.
Each inequality gives us a different upper bound on the number of tuples; chances are that the least upper bound is a good estimate of the number we have in mind.

But why does passing intermediate quantities to entropies help at all if, at the end of the day, we are enumerating a, m, t, and p with and without these inequalities? The answer is that estimating terms like $H(M \mid A)$ only involve two variables, using two layers of for-loops, and so its time complexity is quadratic in the number of audiences/movies/TV series. On the other hand, estimating H(A, M, T, P) involves four variables. So it is beneficial to run additional works, such as estimating $H(M \mid A)$, just so that we have a better idea of how to run the main, quartic work. During this process, understanding Shannon entropy and the Shannon-type inequalities helps us find better executing plans and could save us a lot of time and resources.

Conclusion

Shannon entropy, being essential in communication theory, has surprising applications in fields as far as random number generation and database query optimization.
By understanding and leveraging entropy, we can design more secure cryptographic systems, improve the efficiency of simulations and training, and make better use of computational resources in data processing.
As data-driven decision-making become increasingly important, the foundation of information theory continues to provide valuable insights and practical tools across disciplines.



National Taiwan University
Graduate Institute of Communication Engineering

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

Editor In Chief. Prof. Shih-Chun Lin

Visit Us At. https://gice.ntu.edu.tw/

E-Mail. ntugice@ntu.edu.tw