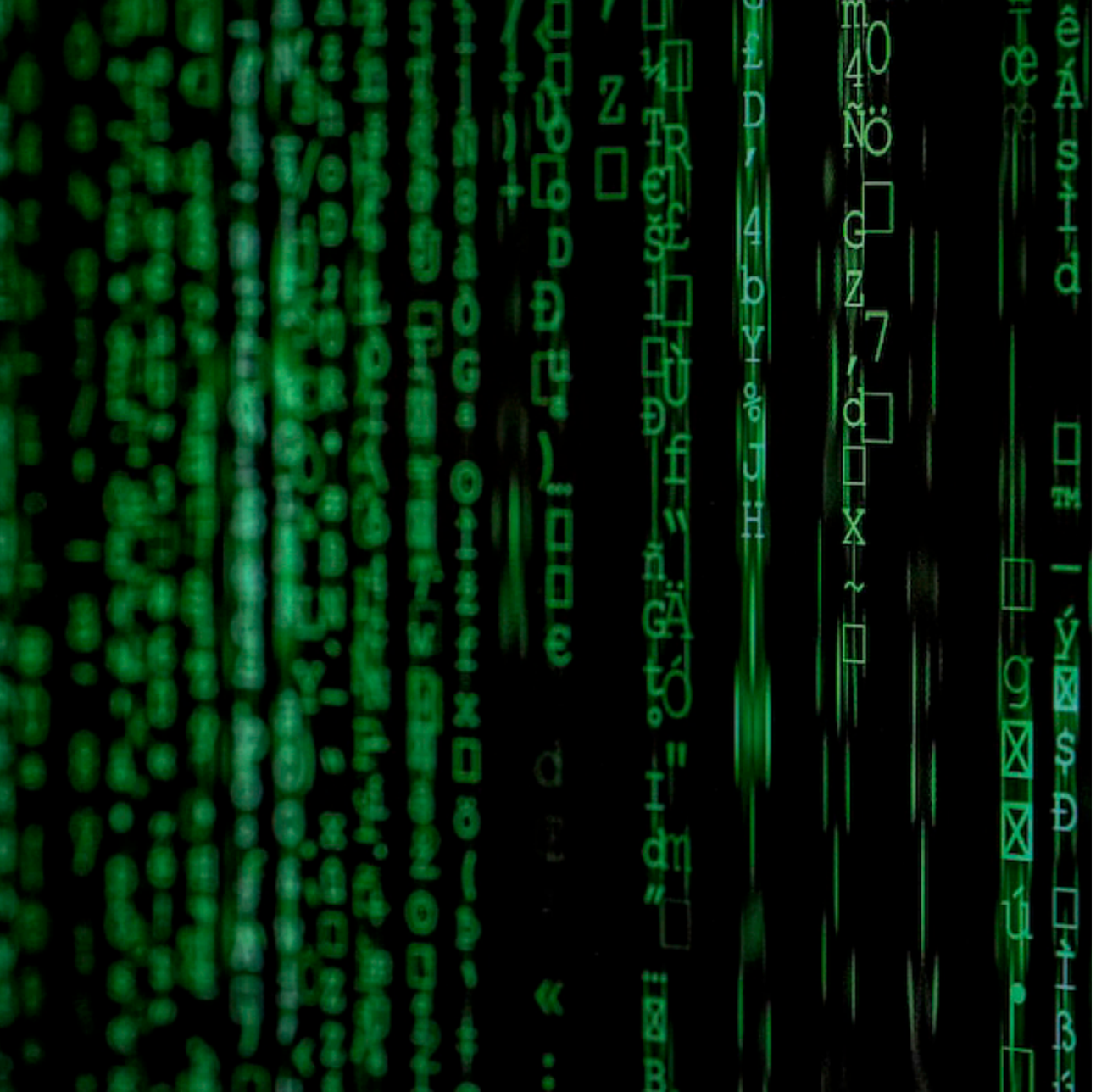
bits

Issue 4 | 2022-2023



FROM THE EDITORS

Dear Reader,

In all the panic and uproar over figuring out what exactly we're going to be doing next year, we finally have some time to really consider how long we've been at Hunter. Six years is a third of our lives. We've seen big sibs, club leaders, captains, peer leaders, mentors, and even friends just a grade above graduate, but leaving has never felt actually real, actually soon until literally right now. What exactly are we going to do in a school where no one understands what the word FLE means? What are we going to do without these locker hallways, our favorite teachers, the stress?

All three of us have been part of bits since the beginning, 2019, four years ago. This is our fourth issue, which means we've made enough bits to get halfway to a byte. We've seen publications rise and publications fall but we hope ours stands the test of time. If all goes according to plan, by 2027 we will have made enough bits to get all the way a byte. But how long would it take to get to a kilobyte? A megabyte? A gigabyte? Well if things continue on this schedule we will reach a kilobyte by the year 10,211, a megabyte by 8,390,627, and a gigabyte by 8,589,936,611. Slightly ambitious if you ask me, but I think we can do it.

We truly want to thank you for supporting this publication, in any form that you have. As small as what you have done may seem to you, you will always be in our hearts. Legacy and the passage of time is such a behemoth to comprehend, but we hope all of you who chose to read this know that you had a massive impact on us, even if we're just a few random people.

We hope that one day, someone is going to look on the bits google drive, see this nerdy letter, and laugh that it says last edited in 2023. We hope you visit us in the metaverse and we promise that when we're super rich one day, we're going to donate a ton to bits.

EICs (Jeffrey Tao, Angela Chan, Olivia Long)

P.S. We'd like to thank our wonderful advisor and computer science teacher, Mr. Cheng, whose support and dedication have helped bring our artistic vision to life. His enthusiasm, expertise, and encouragement inspire us all.

If you're interested in joining the bits community by contributing an article, photographs, or artwork for next year's magazine, please send us an email at bitsmagazinehchs@gmail.com.

bits Magazine

2022-2023

TABLE OF CONTENTS

1. New Developments in Technology

10 Big Data for A Big World, *Logan Reich*

13 Artificial Neural Networks: The Benefit of Sleep Periods, *Caleb Shi*

16 Magnetomicrometry: Where Innovation Attracts, *Angela Wang*

18 ChatGPT: The Newest Advancement in Language Modeling, *Jeremiah Chung*

2. Computer Science in Global News

22 Notion AI, Charlie Tharas

24 Discrimination and Bias in Artificial Intelligence, *Ethan Uppal*

26 Crime Prediction: Revolutionary Breakthrough or Another Fluke?, *Mina Mori*

28 Keeping Rice Nice with Blockchain Technology, *Zhixiao Yip*

30 Artificial Intelligence: The Next Revolution in Medicine?, *Harrison Pratt*

3. Applications of Computer Science

34 The Truth of TouchID: Fingerprint Scanners, *Natalie Viderman*

36 Advancements in Optical Atomic Clocks, *Inika Agrawal*

38 Feistel Ciphers and Symmetric Key Encryption: Protecting Your Data without the Computational Stress, *Victor Robila*

4. Topics in Theoretical Computer Science

42 But What Exactly Is a Bit?, *Ethan Uppal*

44 The K-Nearest Neighbors Algorithm, *Amy Ma*

45 Random Function in Python, *Kaya Parikh*

46 The Leftover Hash Lemma, *Sam Huang*

48 Binary Addition with Logic Gates, *Eden Reinfurt*

50 Finding the Longest Subsequence, *Chloe Zhou*

5. Technicalities, Mechanics, and Tidbits

54 AI Image Upscaling, *Simon Eskin*

56 Looking Backwards, Moving Forwards, *Ian Cho*

59 How to Make Your Website More Accessible for Visually Impaired People, *Alexandra Bernstein*

62 SimplePIR: An Alternative to Google, *Addis Adam*

1. New Developments in Technology

BIG DATA FOR A BIG WORLD

LOGAN REICH

The term “Big Data” has become one of the most popular catchphrases in the media—but what is it really? At its core, Big data is a general term for a dataset, usually with hundreds of thousands, millions, or billions of data points, that needs more advanced analysis than “traditional” data, either because it is large, or because it is more complicated. Common examples of big data include data tracking shipping containers, ocean currents, and political changes. In order to achieve a dataset this big though, data is usually autonomously collected, which is why big data is just starting to bloom in the last 15 years. In addition, automated processes are also needed to deal with every aspect of big data after collection, from data cleaning and processing to analysis and application.

When data scientists assess data’s value , they primarily look at two major categories: variability and veracity. Variability refers to the deviation—or variation—in the data, addressing questions like how frequently the data is measured, how much the data source changes, and how often the data values themselves change. The more variable the data is, the more difficult it is to work with, and generally, the more data points are needed to establish a meaningful trend or conclusion. Veracity, on the other hand, refers to the quality of data. Veracity tackles questions like how accurate the data is, whether the different sources in my dataset measure the same variable using the same metric, and how likely the data is to be biased. Data bias is crucial in data science, since it is hard to get a dataset that accurately represents any quantity one is attempting to analyze. Instead, datasets usually represent a small section of the variable of interest, one that is not guaranteed to accurately reflect the overall data. In order to overcome this bias, one first has to recognize it and then figure out how to correct it.

Besides data bias, another major issue in data science is data anonymization. Many datasets, especially those from healthcare and finance, contain personally identifiable information (PII) that cannot be made available because of privacy concerns. In this case, the data must be anonymized. When thinking of data anonymization, many people imagine simply swapping out names with pseudonyms. Yet data like phone numbers and addresses can also be identifying, meaning they have to be removed too. The only problem with such removals is that, for a lot of data analysis, the data’s geographic distribution is important. Fortunately, data scientists have advanced techniques to overcome this challenge. These include data masking (the modification of sensitive data), generalization (removal of the data’s specificity a, so that it identifies many people instead of one), data swapping (decorrelation of different parts of a dataset, to prevent the use of two non-PII datasets to generate PII), data perturbation (data masking using random noise, which is a set of random numbers that is added to the data), and the use of synthetic data (creating an artificial dataset to mirror the real dataset).

The term “Big Data” has become one of the most popular catchphrases in the media—but what is it really? At its core, Big data is a general term for a dataset, usually with hundreds of thousands, millions, or billions of data points, that needs more advanced analysis than “traditional” data, either because it is large, or because it is more complicated. Common examples of big data include data tracking shipping containers, ocean currents, and political changes. In order to achieve a dataset this big though, data is usually autonomously collected, which is why big data is just starting to bloom in the last 15 years. In addition, automated processes are also needed to deal with every aspect of big data after collection, from data cleaning and processing to analysis and application.

When data scientists assess data’s value , they primarily look at two major categories: variability and veracity. Variability refers to the deviation—or variation—in the data, addressing questions like how frequently the data is measured, how much the data source changes, and how often the data values themselves change. The more variable the data is, the more difficult it is to work with, and generally, the more data points are needed to establish a meaningful trend or conclusion. Veracity, on the other hand, refers to the quality of data. Veracity tackles questions like how accurate the data is, whether the different sources in my dataset measure the same variable using the same metric, and how likely the data is to be biased. Data bias is crucial in data science, since it is hard to get a dataset that accurately represents any quantity one is attempting to analyze. Instead, datasets usually represent a small section of the variable of interest, one that is not guaranteed to accurately reflect the overall data. In order to overcome this bias, one first has to recognize it and then figure out how to correct it.

Besides data bias, another major issue in data science is data anonymization. Many datasets, especially those from healthcare and finance, contain personally identifiable information (PII) that cannot be made available because of privacy concerns. In this case, the data must be anonymized. When thinking of data anonymization, many people imagine simply swapping out names with pseudonyms. Yet data like phone numbers and addresses can also be identifying, meaning they have to be removed too. The only problem with such removals is that, for a lot of data analysis, the data’s geographic distribution is important. Fortunately, data scientists have advanced techniques to overcome this challenge. These include data masking (the modification of sensitive data), generalization (removal of the data’s specificity a, so that it identifies many people instead of one), data swapping (decorrelation of different parts of a dataset, to prevent the use of two non-PII datasets to generate PII), data perturbation (data masking using random noise, which is a set of random numbers that is added to the data), and

FIG. 1

A visualization of big data.

the use of synthetic data (creating an artificial dataset to mirror the real dataset).

One of the largest difficulties with big data, though, is how it's obtained in the first place. In almost all cases, the process involves building a network of low-cost data gathering sensors, which can range from credit card terminals to home air quality sensors and small satellites, and connecting them to the Internet for automatic data amalgamation. Often these sensors come from the Internet of Things, the wide collection of relatively low-cost Internet-connected sensors available in the modern age. Big data can also be gathered through manual entry, such as in medical record updates or shipping manifests. Only once data has been collected can it be anonymized, assessed for veracity and variability, cleaned through outlier and bias removing techniques that are often dataset specific, and then finally transferred for usage.

So what is big data actually useful for? Well, in some sense, everything. Big data can be used to create key tracking metrics assessing macroscopic trends, like how the economy is doing, what climate change looks like, and how diverse neighborhoods are. It can also predict how these trends evolve over time. Big data can also be used to train machine learning (ML) algorithms to perform a wide number of tasks, such as identifying hot dogs, performing facial recognition log-ins, and improving traffic light timings. Many of the advances in machine learning, and computer science in general, either rely on optimizing algorithms handling big data, use big data to train a model, or use big data in the model itself!

Many people are scared by the possibility of their personal data being used by large organizations for seemingly-mysterious purposes, causing them to be scared of big data itself. However, the reality is that almost all data scientists don't want to use data for nefarious purposes—they just want their models to work. Big data has enormous possibilities, and as long as we're careful and ethical with our data anonymization, application, and bias removal, it can lead to a big future.

REFERENCES

Bernstein, C. (2021, September 24). What is pii (personally identifiable information)? definition from searchsecurity. SearchSecurity. Retrieved November 17, 2022, from https://www.techtarget.com/searchsecurity/definition/personally-identifiable-information-PII

Big data: What it is and why it matters. SAS. (n.d.). Retrieved November 17, 2022, from https://www.sas.com/en_us/insights/big-data/what-is-big-data.html

Data Anonymization: Use Cases and 6 common techniques. Satori. (2022, July 14). Retrieved November 17, 2022, from https://satoricyber.com/data-masking/data-anonymization-use-cases-and-6-common-techniques/

Cepero, R. (2019, December 29). 5 Biggest Big Data Challenges. Bleuwire. Bleuwire. Retrieved April 22, 2023, from https://bleuwire.com/5-biggest-big-data-challenges/

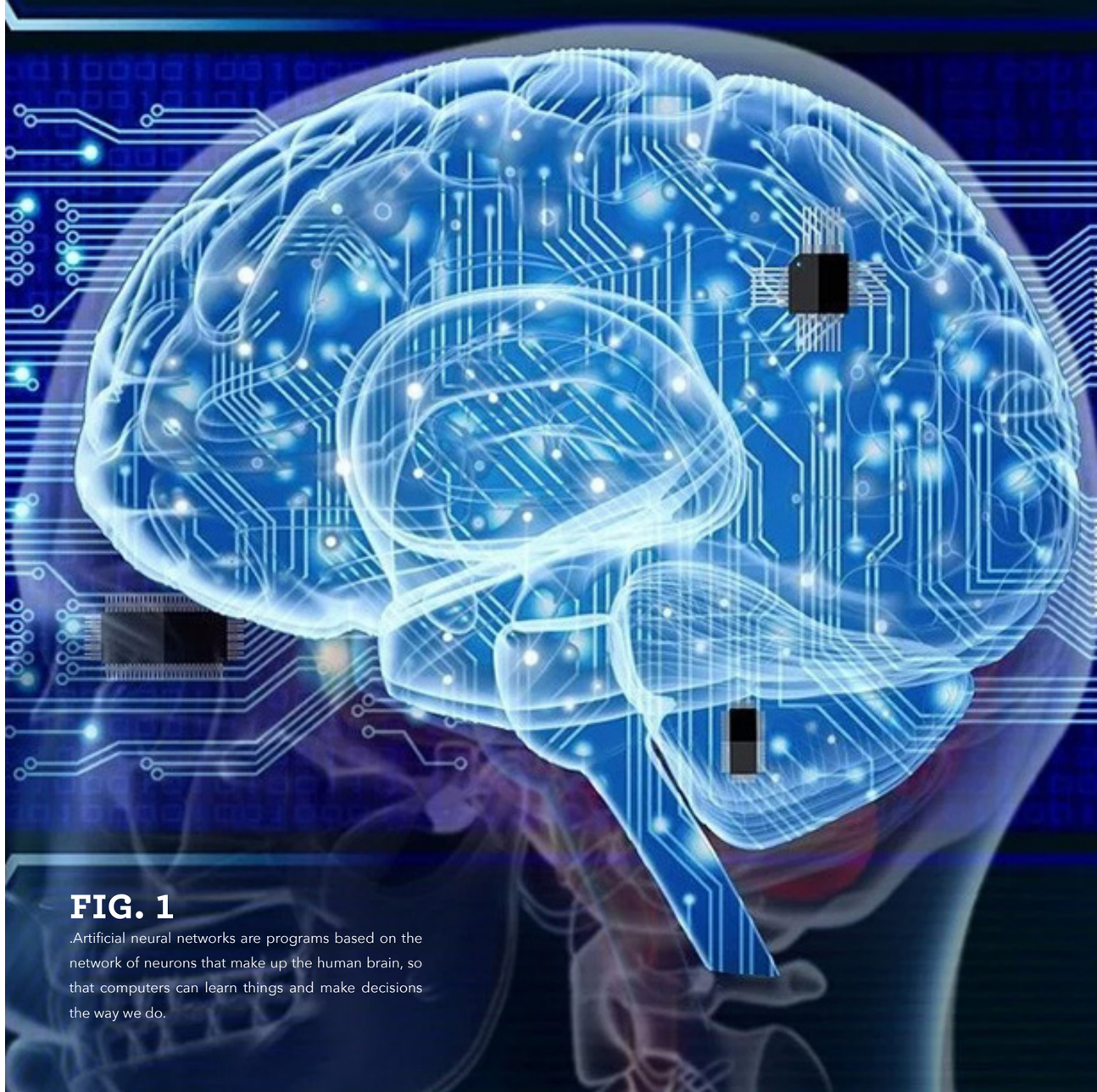


FIG. 1

.Artificial neural networks are programs based on the network of neurons that make up the human brain, so that computers can learn things and make decisions the way we do.

ARTIFICIAL NEURAL NETWORKS

The Benefit of Sleep Periods

CALEB SHI

The idea of artificial neural networks was first proposed in 1944 by Warren McCullough and Walter Pitts, two researchers at the University of Chicago, who would subsequently go on to found the first cognitive science department at MIT in 1952. A subset of machine learning, artificial neural networks involve a computer learning to perform a task by analyzing training samples that are usually hand-labeled in advance. For example, an object recognition system might be given thousands of labeled images of cars, houses, and other items to find visual patterns in the images that consistently correlate with particular labels. However, artificial neural networks go beyond machine learning: they are programs modeled after the neural network making up the human brain, so that the computers can learn and make decisions as we do. Typically, these networks consist of dozens to millions of artificial neurons, called units, arranged in three layers: input, hidden, and output. The input layers receive various forms of information from the outside world, which they aim to process and learn about. Afterwards, the data goes through one or more hidden layers so that it can be transformed into something the output layers can use. Finally, on the other side of the network, the output layers respond to the data it was given and processed. Since artificial neural networks are fully connected from one layer to another, Data moves through different layers, and the network learns more about the data at each layer.

One significant challenge that researchers face when creating artificial neural networks is a phenomenon called catastrophic forgetting, where new information overrides old information as the networks learn sequentially,. But Dr. Maxim Bazhenov, a professor of medicine and a sleep researcher at UC San Diego's School of Medicine, has a solution: spiking neural networks. Spiking neural networks artificially mimic natural neural systems by transmitting information as discrete events, or spikes, at certain time points instead of continuously. During Dr. Bazhenov's research, when the spiking networks were trained on a new task with occasional offline periods that mimicked sleep, catastrophic forgetting was drastically mitigated. Similar to the human brain, sleep for the networks allowed them to replay old memories without explicitly using old training data. Ultimately, new developments in computational biology have utilized biological models to help reduce the threat of catastrophic forgetting in artificial neural networks, which can benefit a wide variety of research interests, especially ones concerning memory loss such as aging, neurodegenerative conditions such as Alzheimer's, and so on.

REFERENCES

Hardesty, Larry. "Explained: Neural Networks." MIT News, April 14, 2017. https://news.mit.edu/2017/explained-neural-networks-deep-learning-0414.

LaFee, Scott. "Artificial Neural Networks Learn Better When They Spend Time Not Learning at All." UC

San Diego Today, November 18, 2022. https://today.ucsd.edu/story/artificial-neural-networks-learn-better-when-they-spend-time-not-learning-at-all.

Marr, Benard. "What Are Artificial Neural Networks - A Simple Explanation For Absolutely Anyone."

Forbes, September 24, 2018. https://www.forbes.com/sites/bernardmarr/2018/09/24/what-are-artificial-neural-networks-a-simple-explanation-for-absolutely-anyone/?sh=58c10eaf1245.

University of California - San Diego. "Artificial neural networks learn better when they spend time not learning at all: Periods off-line during training mitigated 'catastrophic forgetting' in computer systems." Science Daily, November 18, 2022. https://www.sciencedaily.com/releases/2022/11/221118160305.htm.

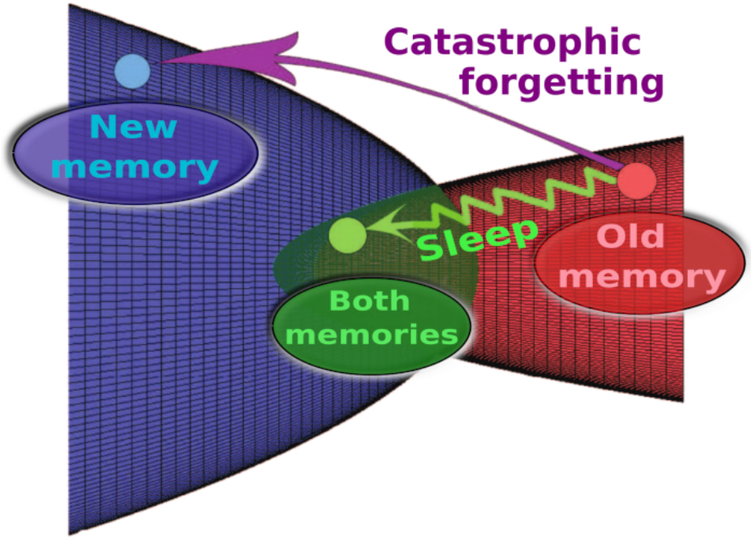


FIG. 2

In artificial neural networks, new information can override old information, a phenomenon called catastrophic forgetting. Dr. Maxim Bazhenov's team found that periods of sleep can consolidate old memories with new ones, without any loss of learning.

MAGNETOMICROMETRY

Where Innovation Attracts

ANGELA WANG

It's August 18, 2021, and scientists at MIT's Media Lab have finally developed a new method of controlling prosthetic limbs. Called magnetomicrometry (MM), the technique allows scientists to use small magnetic beads to send computer models specific information on the length and speed of a patient's muscle contraction within milliseconds, allowing the person to control prosthetic limb movements more fluidly and naturally.

Previous approaches to controlling artificial limbs had largely involved electromyography, which measures electrical activity from the muscles using electrodes either attached to the surface of the skin or surgically implanted in the muscle. However, this technique is highly invasive, expensive, and provides limited information about muscles. By transmitting only intermediate signals between the brain and muscle rather than information about the actual contractions in the muscle, not much is learned about how the muscle is intended to behave, thus affecting the effectiveness of the prosthetic limbs.

MIT's use of magnetic sensors serves to counter this issue: by placing pairs of magnets into the muscle tissue around the amputated area, the researchers can measure the movements of the magnets in relation to each other through mobile sensing-arrays and determine how much the muscles are contracting, as well as how quickly (Fig. 1). Aside from being incredibly accurate, MM has also been proven to be minimally invasive without the need for replacement for a lifetime.

Hugh Herr, the professor at the head of the Biomechatronics group in the Media Lab and senior author of the paper, and Cameron Taylor, an MIT postdoc and the study's lead author, had constructed an algorithm two years ago that decreased the amount of time necessary for the sensors to determine the positions of the magnets, allowing MM to be more rapid. The researchers tested their algorithm on the calf muscles of turkeys, placing the 3-millimeter magnets 3 centimeters apart on the outside of their legs. They were able to achieve an accuracy of 37 microns—the width of a human hair—in determining the location of the magnets in just 3 milliseconds as they shifted the turkeys' ankle joints.

In order to control a prosthetic limb, a computer model uses the muscle contractions to determine where the patient's prosthetic would be, allowing the patient to move their limb where they want. Researchers are then able to determine the target positions and speeds of prosthetic joints using mathematical models and use a simple robotic controller to execute them.

In the future, the researchers hope to conduct a small study on human patients with amputations below their knees using sensors that can be attached to clothing, the surface of the skin, or outside a prosthesis. They seek to use MM to improve muscle control through functional electrical stimulation, which involves applying small electrical currents to a paralyzed or weakened muscle and currently helps people with spinal cord injuries with mobility. Another direction they hope to take their project in is in guiding robotic exoskeletons, which can be affixed to any joint to aid people with a stroke or other muscle weakness. This application can amplify the action of biological muscles in stroke-impaired limbs. With the numerous applications of MM, the future is magnetic.

REFERENCES

"Functional Electrical Stimulation (FES)." MS Trust. Multiple Sclerosis Trust, last modified March 1, 2020. https://mstrust.org.uk/a-z/functional-electrical-stimulation-fes.

Trafton, Anne. "Magnets Could Offer Better Control of Prosthetic Limbs." MIT News. Massachusetts Institute of Technology, August 18, 2021. https://news.mit.edu/2021/magnet-prosthetic-limb-control-0818.

Taylor, Cameron. "Magnetomicrometry-Based Control." MIT Media Lab. August 18, 2021. Video, 2:35. https://youtu.be/bU2jEA6u2rk.

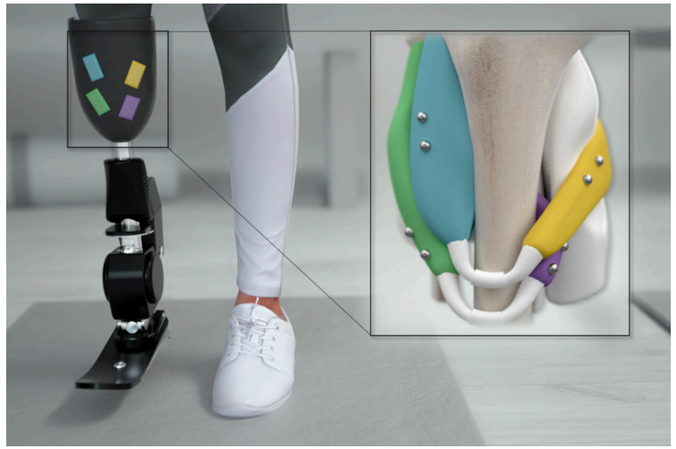


FIG. 1

A view of magnetomicrometry in a prosthetic limb. The left shows the multiple mobile-sensing arrays that help track tissue strain; the right shows a zoomed-in view of the pairs of magnetic beads used to track these movements.

CHATGPT: THE NEWEST ADVANCEMENT IN LANGUAGE MODELING

JEREMIAH CHUNG

The Chat Generative Pre-trained Transformer, more commonly known as ChatGPT, has been a subject of controversy in recent months. The chatbot was developed by OpenAI, a leading AI research institute. One of the most advanced language models to ever be created, ChatGPT pulls and analyzes information from all across the internet to learn and replicate the nuances of human language. Although it is already capable of generating grammatically correct, contextually relevant, and factually accurate responses, ChatGPT continues to learn, adapt, and optimize its performance based on user inputs.

What sets ChatGPT apart from earlier, less advanced chatbots is how its understanding of natural language frees it from relying on constricting rules and scripted responses, which allows it to simulate impressively realistic conversations that are tailored to the unique situations it is presented with.

Though ChatGPT has convincingly demonstrated the practical possibilities of AI in improving the quality of life and the efficiency of those working in industries ranging from customer service to education, many are also concerned with the revolutionary tool's uncanny ability to write convincingly human text. This concern has unfortunate merit, especially as ChatGPT continues to improve—its unprecedented understanding of and therefore capacity to reproduce human-sounding text is a major concern, as it can empower misuse ranging from plagiarism to misinformation.

This unease seems to be especially present among educators, who fear ChatGPT will be used to complete their assignments, rendering them worthless for teaching students. Some have made the decision to completely phase out certain writing assignments because of ChatGPT's ability to respond to specific prompts accurately, inconspicuously, and instantaneously.

Despite the hesitancy of some to embrace tools like ChatGPT, it undeniably represents a breakthrough in AI technology. This innovation has demonstrated the practical potential of ChatGPT, and its increasing role in our lives. With consistent careful development, AI technology such as ChatGPT may very well prove to reshape the way humans and machines interact.

REFERENCES

OpenAI, O. A. I. (2022, November 30). CHATGPT: Optimizing language models for dialogue. OpenAI. Retrieved February 23, 2023, from https://openai.com/blog/chatgpt.

2. Computer Science in Global News

PRODUCT REVIEW: NOTION AI

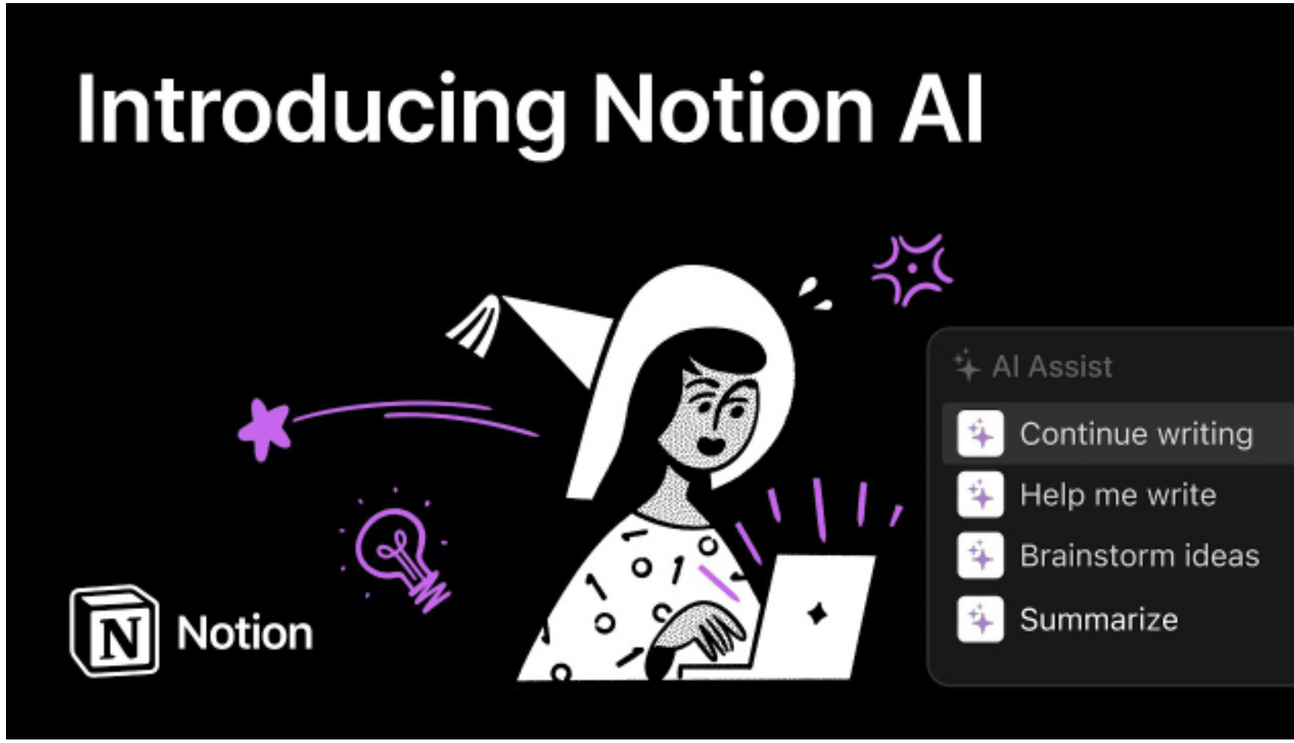
CHARLIE THARAS

For Hunterites struggling under the crushing weight of demanding coursework, extracurricular responsibilities, family obligations, and exhausting hobbies, the white alphabet block logo of Notion is often a welcome sight. The app's clean, minimalist interface is built for collaborative projects, task tracking, and notetaking—which is why it came as a surprise to some when Notion's team unveiled Notion AI, a writing assistant integrated with the Notion platform. What did Notion's aesthetically pleasing to-do lists have to do with AI?

It turns out that the connections are more intuitive than one might expect. Notion's AI is portrayed (like most AI writing software) as an "assistant" designed to tackle the menial tasks of writing, particularly in corporate settings. When users select the AI command in-app, they're presented with the ability to create AI-generated pros and cons lists, outlines, meeting notes, and sales emails along with unexpectedly creative options: poems, creative stories, and blog posts are interspersed with corporate suggestions. At first glance, these might elicit concerns from those in academic spaces worried about plagiarism and other forms of cheating. However, unlike many other AI writers, Notion AI's "assistant" approach seems to actually work for one simple reason: it kind of sucks.

When asked to describe itself, Notion AI lists features that it does not even remotely possess, such as "customer journey optimization" and "predictive analytics." It is buzzword-prone and significantly more factually incorrect than other popular AI writers. Generated essay outlines are extremely generic, no matter the topic inputted to the AI prompt, with suggestions to "reflect on the essay's topic" in the conclusion. Strangely, the only tasks the AI seems to perform competently are creative stories, which are often even more fantastical than those of the infamous ChatGPT.

While Notion has yet to release specifics on the technology powering its AI, it's reasonable to assume that the relatively small San Francisco-based company—which has little to no experience in the AI field and specializes in virtual workspaces—has fewer resources to throw around at cutting-edge natural language processing than companies like Microsoft-backed OpenAI, which is currently valued at nearly $30 billion. Perhaps, though, the AI's skill levels are at least partially intentional: maybe Notion truly means to develop an assistant and not a replacement. Either way, for students conflicted about the ethics of using ChatGPT, I wholeheartedly recommend Notion AI: it's bad enough to keep you working honestly.



The thumbnail to the Notion AI introduction video.
Source: YouTube/Notion

Fig. 1

REFERENCES

Notion, "Introducing Notion AI," YouTube Video, 1:24, November 16, 2022, https://www.youtube.com/watch?v=FElBbgnNtVA

Cao, Sissi. "OpenAI, the Company behind CHATGPT, Is Valued at $29 Billion." Observer, January 6, 2023. https://observer.com/2023/01/chatgpt-openai-valued-29-billion/.

These charts show that scores for white defendants were skewed toward lower-risk categories. Scores for black defendants were not.

FIG. 1

DISCRIMINATION AND BIAS

in Artificial Intelligence

ETHAN UPPAL

Too often, the debate about artificial intelligence and machine learning (read my Radicals article for the calculus behind AI!) only considers the ethical and theoretical implications of doomsday scenarios or human displacement without addressing the real problems we face today. Machine learning models are deployed at this very moment to determine whether someone receives a certain advertisement, gets employed, or remains incarcerated.

I will not waste my precious few words on fluff. Prisons and courtrooms use algorithms to determine a defendant's or inmate's risk, and their judgments are very often skewed in favor of white people. A ProPublica investigation found that "black defendants were still 77 percent more likely to be pegged as at higher risk of committing a future violent crime and 45 percent more likely to be predicted to commit a future crime of any kind." In an even more unsavory case, researchers Julia Dressel and Hany Farid found that COMPAS, a widely used package for predicting whether a criminal will recommit crimes, "is no more accurate or fair than predictions made by people with little or no criminal justice expertise," and that "despite COMPAS's collection of 137 features, the same accuracy can be achieved with a simple linear classifier with only two features."

Hiring often employs AI as an aid, which if the findings above are anything to go by, one would expect to end in disaster. That is exactly what happened when Amazon tried to use a résumé classifier. Unsurprisingly, the company found that the classifier favored men. It had been trained on the past ten years of résumés, most of which belonged to men. We expect our AI gods to rise above our moral lowliness, but we forget that all models are trained on data—human data—which contains all our biases and flaws.

REFERENCES

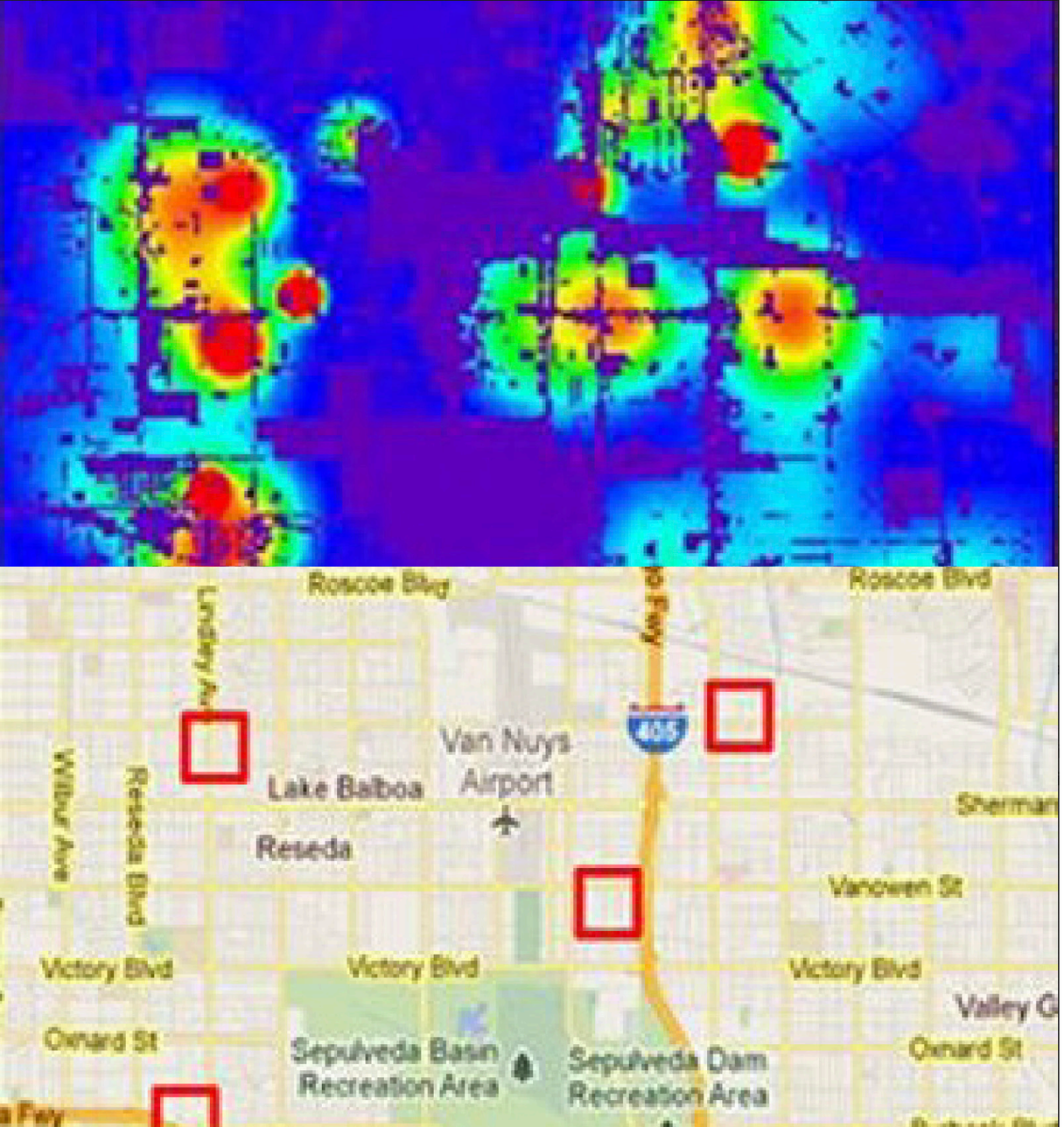
https://www.khanacademy.org/computing/ap-computer-science-principles/data-analysis-101/x2d2f703b37b450a3:machine-learning-and-bias/a/bias-in-predictive-algorithms

https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

https://www.science.org/doi/10.1126/sciadv.aao5580 https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G

https://arxiv.org/abs/1806.06301

https://qz.com/1427621/companies-are-on-the-hook-if-their-hiring-algorithms-are-biased/



CRIME PREDICTION

Revolutionary Breakthrough or Another Fluke?

MINA MORI

How can we predict a crime that hasn't been committed yet? A question straight out of Steven Spielberg's famous sci-fi drama, ***Minority Report***. However, instead of three strange "precog" mutants predicting the future with their advanced brains, modern crime rate prediction is based on algorithms that use data to recognise patterns in time and location to forecast crimes. In some societies with high crime rates, predicting crime may become an important development in police networking.

The main approach to crime rate prediction is to use a specific type of machine learning (ML), which generally allows a system to learn and improve based on past experiences. ML includes algorithms such as a k-nearest neighbor (KNN) algorithm (using proximity to predict the groupings of an individual data point) and linear regression to convert datasets from previous years into predictions based on the type, location, and time of the crime. Figure 1 shows a prediction made using machine learning in a portion of Van Nuys, California. The left image shows the predicted areas of crime hotspots, while the right depicts the full map, with the boxes representing the crime hotspots based on retrieved data.

However, the data that is used to train this technology may be skewed because of biased police responses. This idea could work well in a society with completely unbiased personnel, but unfortunately, such a society does not exist. Additionally, crimes are not guaranteed to occur in the said "hotspots," as past trends are not a guaranteed predictor of future action.

Although we cannot predict exact crimes such as in Minority Report, the probability of a crime occurring in a certain place at a specific time can help police to keep cities and neighborhoods safe!

REFERENCES

Wood, M. (2022, June 30). Algorithm predicts crime a week in advance, but reveals bias in police response. Biological Sciences Division | The University of Chicago. Retrieved March 9, 2023, from https://biologicalsciences.uchicago.edu/news/features/algorithm-predicts-crime-police-bias

"Crime Rate Prediction Using K Means." Nevon Projects, December 20, 2022. https://nevonprojects.com/crime-rate-prediction-using-k-means/#:~:text=Data%20mining%20algorithm%20will%20extract,which%20will%20occur%20in%20future.

Shah, Neil, Nandish Bhagat, and Manan Shah. SpringerOpen. Springer Singapore, April 29, 2021. https://vciba.springeropen.com/articles/10.1186/s42492-021-00075-z.

"Machine Learning Report - University of Pennsylvania." Accessed March 9, 2023. https://www.seas.upenn.edu/~tabedzki/machine-learning-report-final.pdf.

Sharma, Shivam. "Crime Rate Prediction." Medium. Medium, August 29, 2021. https://medium.com/@sshivam6535/crime-rate-prediction-f4d9255067e0.

KEEPING RICE NICE WITH BLOCKCHAIN TECHNOLOGY

ZHIXIAO YIP

The staple that feeds over 3.5 billion people on Earth, rice growth alone touches a stunning 122 different countries. But for the most part, research has been focused on ways of rice-planting to increase yield, rarely venturing beyond that. As such, problems like heavy metal and pesticide pollution, as well as the use of excessive additives, are often overlooked in research. Addressing the problem, though, came down to increasing legal-awareness and establishing supervisable standards for governments–highly labor and material intensive options that also fail to address the dynamism of circulating rice. In addition, their centralized methods of data storage, putting all their data in a specific bank or database, makes them vulnerable to tampering and loss. A new system promises to change that.

Using blockchain technology, a platform where the emphasis is on decentralization itself, scientists were able to create smart contracts for the rice–bits of code that run and self-check automatically. Meanwhile, the blockchain itself ensures the security of the smart contract code, letting different bits of code jointly maintain data security, which traces the entire data chain when it comes to storage. These small, automated control pieces can then combine to give companies internal management and data interconnection functions – constantly looking at the regulators all along the supply chain –enabling them to hold supervisors accountable while giving consumers services like rice traceability.

The scientists' current smart contracts specifically deal with automatic data collection along the entire rice life-cycle. One group of contracts monitors information on harmful pollutants, seed sources, hygiene, as well as transportation and storage logistics in the supply chain. Meanwhile, the second group monitors the behavior of companies, consumers, and regulators to hold people accountable. Organized into a series of modules – initialization, supervision, storage – with categories nested within one another, the data is stored and recalled through a blockchain cloud database. The scientists then repeatedly used the model during design to ensure its accuracy.

Blockchain technology has already been seen in places like Bitcoin. But now, in addition to keeping your cryptocurrency safe, it can also tell you how safe the food you eat is.

REFERENCES

"Food Staple." National Geographic Society. Accessed January 31, 2023. https://education.nationalgeographic.org/resource/food-staple.

Peng, Xiangzhen, Xin Zhang, Xiaoyi Wang, Haisheng Li, Jiping Xu, and Zhiyao Zhao. "Construction of Rice Supply Chain Supervision Model Driven by Blockchain Smart Contract." Scientific Reports 12, no. 1 (2022). https://doi.org/10.1038/s41598-022-25559-7.

FIG. 1

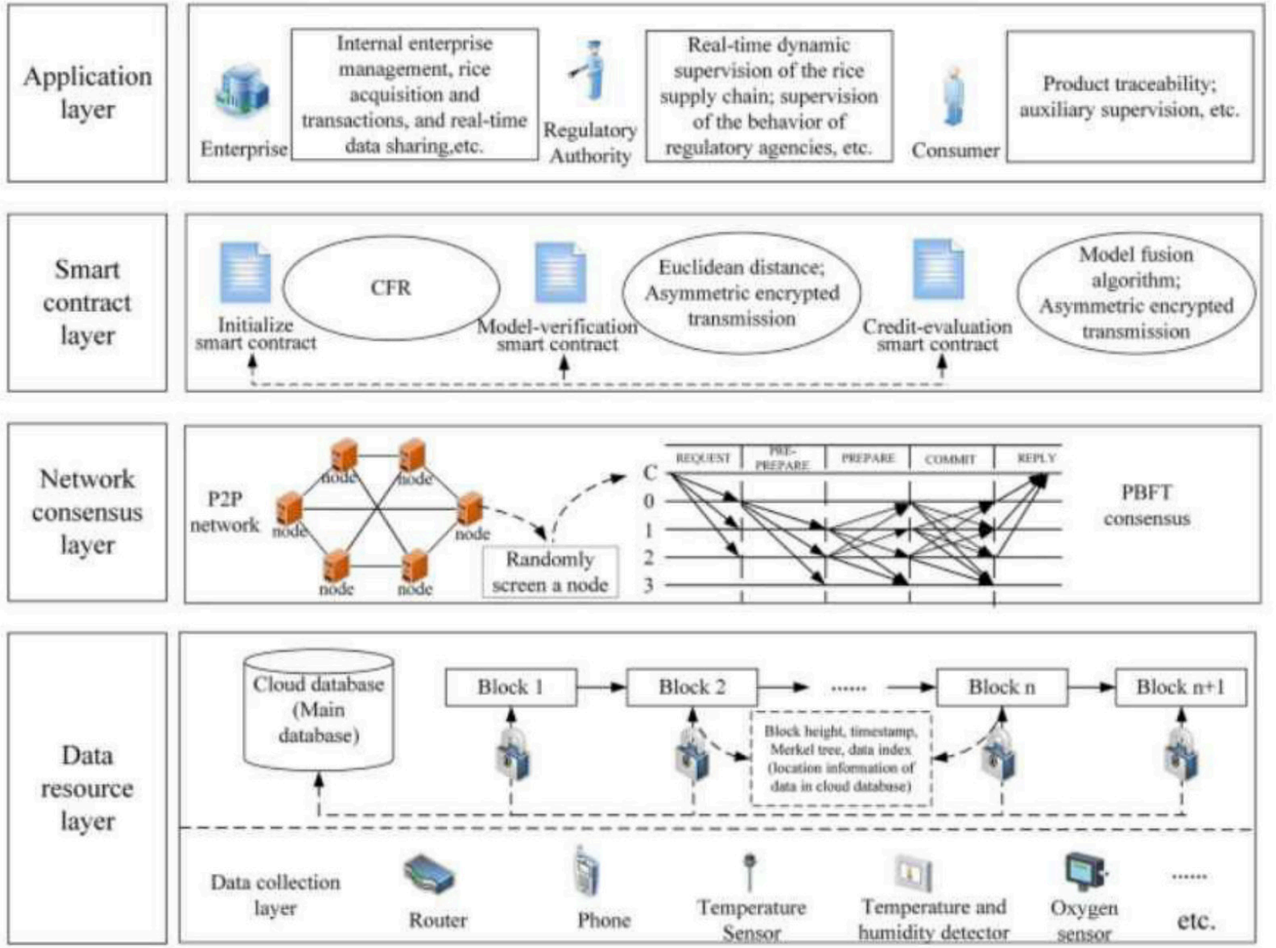
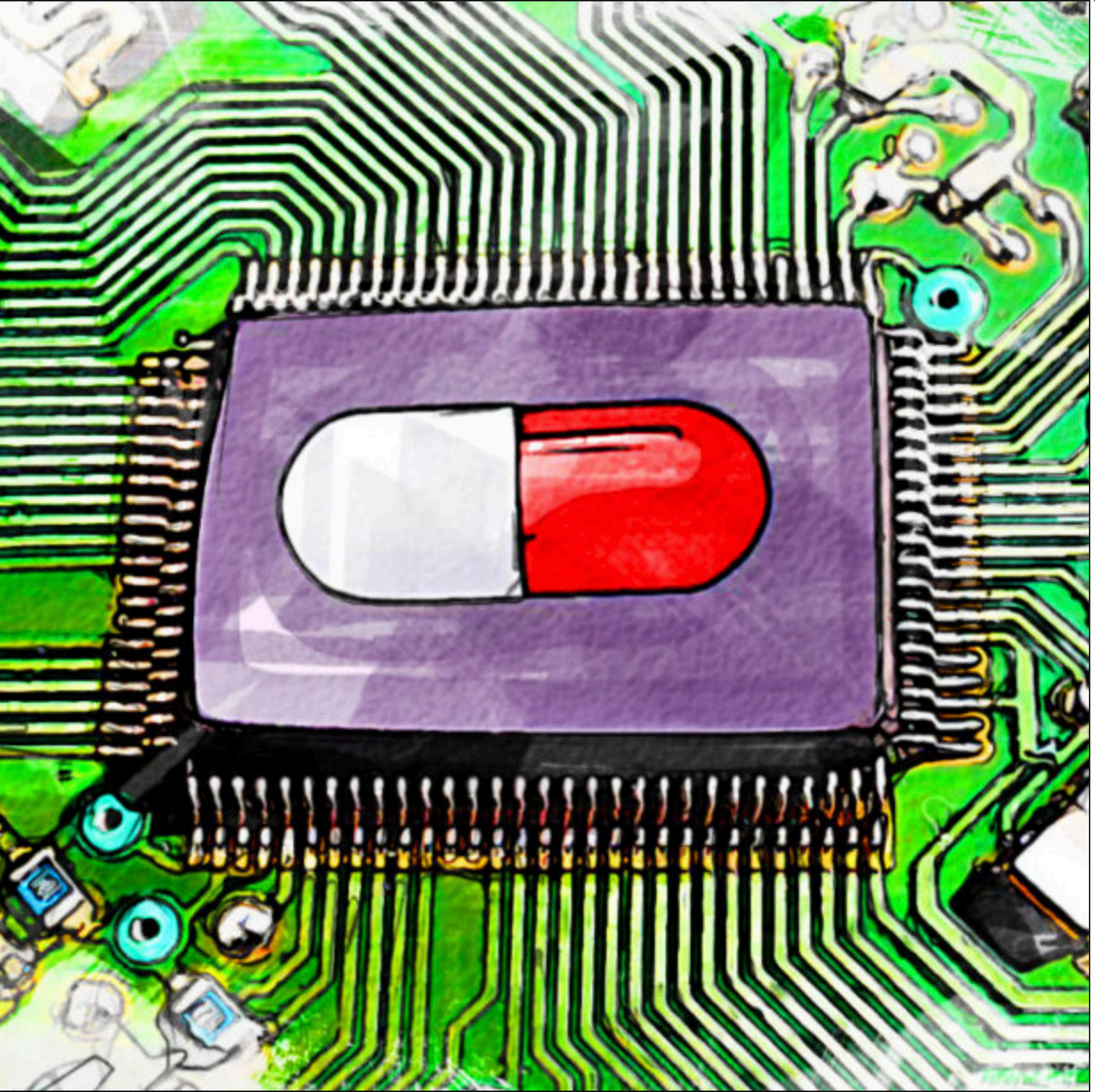


Image of organization levels involved in the scientists' rice-supply management system.
Image and caption: Peng et al., 2022



ARTIFICIAL INTELLIGENCE

The Next Revolution in Medicine?

HARRISON PRATT

Artificial intelligence is a rapidly growing field of computer science, touching everything from visual art to essay writing. With the massive potential of artificial intelligence, many have wondered whether the next step in medical drug development will be born out of this field.

In recent years, the use of artificial intelligence to increase the efficiency of bringing medicines to market has been on the rise. Artificial intelligence programs are currently being trained to organize and streamline the analysis of the overwhelming amounts of data that are collected during clinical testing. This data can range from measured side effects to treatment efficiency compared to prior results. Analyzing and forming conclusions out of the data collected in test trials requires massive amounts of calculations, and hours upon hours of human labor. As posited in an article by Pfizer describing the use of artificial intelligence in medical development, AI currently serves as something of a "super-intern." While not thinking or making decisions on its own, AI programs crunch the numbers and pick out the most valuable data. With this information, scientists can make quicker and more informed decisions about continued drug development.

However, simplifying drug development is just the tip of the iceberg in the eyes of many hopeful scientists. Many believe that the discovery of new drugs can be initiated by AI programs. Research is being conducted into using AI to this extent in drug development, including by a team from Harvard Medical School. The study is aiming to address the issue of the massive time span (11 to 16 years on average) and cost (close to between 1 and 2 billion on average) of medical drug developments. It is extremely difficult to determine whether promising chemical compounds in a laboratory will have the intended effects in actual medical practice. There are roughly 10 to the power of 60 small chemical compounds, and very few are capable of positive medical effects. Using AI will hopefully be able to find which of these compounds would be safe and effective in human therapies before testing, and allow the research process into the vast amount of compounds to be far more focused and effective. This specific study is attempting to train AI to recognize patterns in known subsets of chemicals, analyzing the data set for chemicals with similar patterns and attempt to predict the effects. Currently, the researchers are testing their programs on baseline, simple data sets. They eventually hope for these programs to be able to work on much more complex data sets, but for now, the progress of researchers is encouraging for the future of drug discovery through AI programs.

REFERENCES

"Artificial Intelligence: On a Mission to Make Clinical Drug Development Faster and Smarter." Pfizer. Accessed February 25, 2023. https://www.pfizer.com/news/articles/artificial_intelligence_on_a_mission_to_make_clinical_drug_development_faster_and_smarter.

Paul, Debleena, Gaurav Sanap, Snehal Shenoy, Dnyaneshwar Kalyane, Kiran Kalia, and Rakesh K Tekade. "Artificial Intelligence in Drug Discovery and Development." Drug discovery today. U.S. National Library of Medicine, January 2021. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7577280/.

Pesheva, Ekaterina. "Can Ai Transform the Way We Discover New Drugs?" Can AI transform the way we discover new drugs? | Harvard Medical School, November 17, 2022. https://hms.harvard.edu/news/can-ai-transform-way-we-discover-new-drugs.

3. Applications of Computer Science

THE TRUTH OF TOUCH ID

Fingerprint Scanners

NATALIE VIDERMAN

We've all experienced biometrics before, from the fingerprint scanner on our computers to the Face ID on our iPhones. It's become an essential part of our lives and allows us to forget about the dozens of different passwords we have. But in a world where we're becoming more and more dependent on technology every day, we need to know more about the technology that knows everything about us.

Biometrics are unique physical characteristics that can be used for automated recognition. Some types of biometrics include fingerprint, face, DNA, and ear recognition, which we all have unique identifiers for. Every type of biometric works differently, but they all analyze a certain part of your body to ensure that the person claiming to be you actually is you. It is difficult to explain all of the many complex types of recognition, so this article will focus on the type of recognition used most frequently- fingerprinting.

It is a well-known fact that every person's fingerprint is unique, but how? This can be explained based on how fingerprints are made. A human fingerprint is usually formed by the seventh month of fetus development and is dependent on the genetic code and several environmental factors, like the position in the womb and the density of the amniotic fluid. All of these factors are so random that it is impossible for any two humans to have identical fingerprints—even for twins.

Every sensor starts out by mapping out the fingerprint. In a process known as capacitive minutia mapping, the sensor analyzes specific points called minutia points on your fingerprint that are turned into a map, which is then converted into a data stream for the sensor to store. Every time a new fingerprint touches the sensor, a new map is created, and if the data stream matches the stream that's already stored within the sensor, then the fingerprint is the same and can be authorized. However, the way that this map is created depends on the software behind the fingerprint sensor. The three main types of software are optical, capacitive, and ultrasonic.

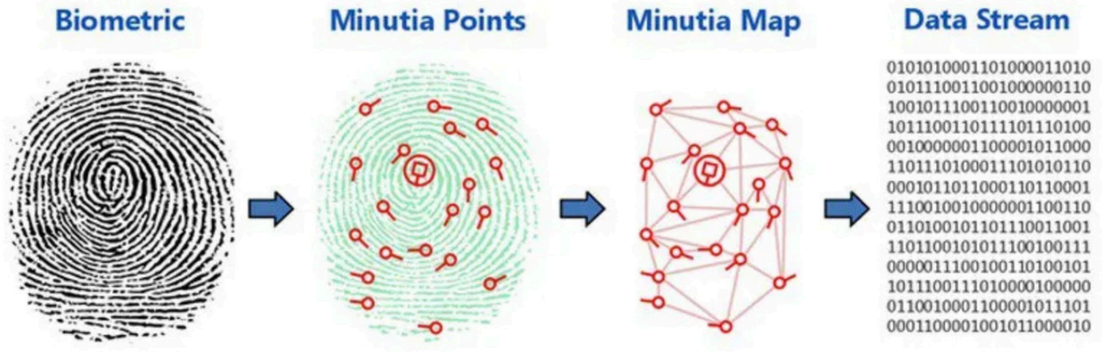


FIG. 1

An optical fingerprint sensor does exactly what it sounds like—it takes a very high-quality photo of the fingerprint and stores that photo. Every time a new fingerprint is scanned, it cross-references that photo with the stored photo. However, this software isn't very accurate because of how easy it is to trick. Anything from an artificial finger to a high-quality image can fool this type of sensor.

On the other hand, capacitive scanners are harder to fool because they require a live finger to scan the fingerprint. Every fingerprint has multiple ridges, lines, and valleys. Hundreds of tiny capacitors lie on the sensor. The distance between a ridge and capacitant—the electrical device in a fingerprint scanner—is not very long, whereas the distance between a valley and capacitant is long because of the air gap in between. Each of these distances and lengths is then passed onto an operational amplifier, which produces a digital scan of the fingerprint. The only way to bypass these scanners is to actually hack the device, because an image will not have capacitor abilities, and a prosthetic finger cannot directly imitate the touch capacitance of an actual finger because it is unique to a live finger.

The final and most advanced type of fingerprint scanner is the ultrasonic type. An array of ultrasonic transmitters and receivers emit ultrasonic pulses that are reflected by the ridges and valleys of the fingerprint. This complex technique allows the scanner to create a 3D scan of the fingerprint. The scans often take a long time to complete but are easy to implement. Because of their advanced technology, they are the most robust method as the only way to bypass them is through advanced hacking.

As we store more of our personal data on the technology all around us, we have to understand the ways it's being kept secure. The next time you're using Touch ID on your iPhone, consider the myriad of technology underneath the capacitive sensor and how it's keeping all of your data safe.

REFERENCES

Agnihotri, Nikhil. n.d. "What are the different types of fingerprint scanners?" Engineers Garage. Accessed April 13, 2023. https://www.engineersgarage.com/different-types-fingerprint-scanners-optical-capacitive-ultrasonic-in-display/.

Hsu, David S. 2016. "Fingerprint Sensor Technology And Security Requirements." Semiconductor Engineering. https://semiengineering.com/fingerprint-senor-technology-and-security-requirements/.

"Types of Biometrics." n.d. Biometrics Institute. Accessed April 13, 2023. https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/.

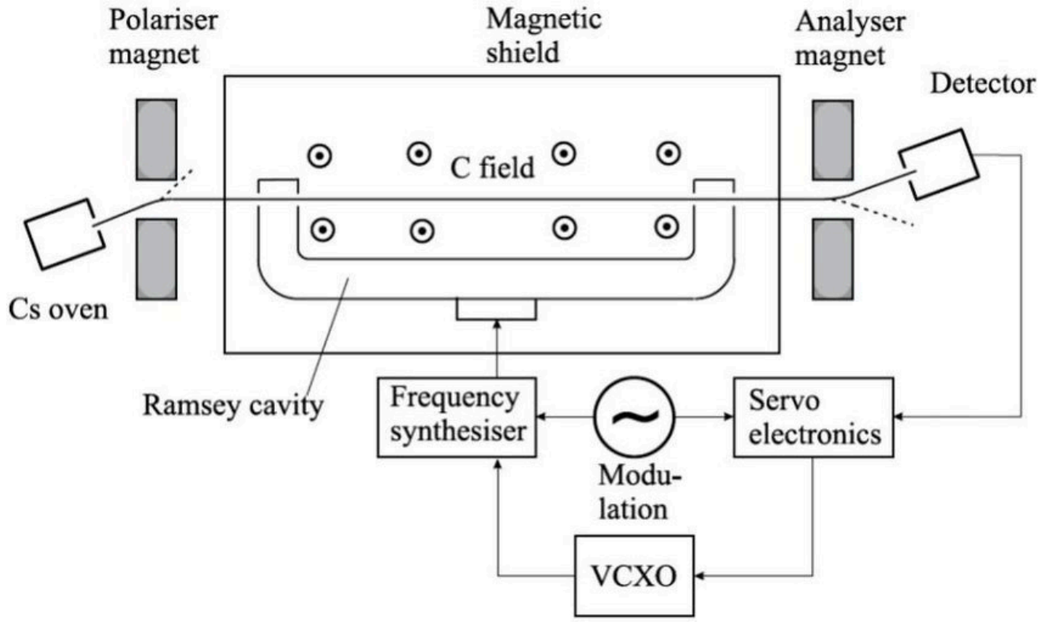


FIG. 1

A block diagram of a cesium-based atomic clock.

ADVANCEMENTS IN OPTICAL ATOMIC CLOCKS

INIKA AGRAWAL

In areas of study where the accuracy of time is extremely important, like space exploration and navigation systems, atomic clocks allow for a much more exact measurement of time than common quartz crystal clocks. Atomic clocks work by combining a quartz crystal oscillator with a collection of atoms, and then using a microwave to create a jolt of energy that moves the electrons in each atom to a higher orbit around the nucleus. The measured frequency needed for these microwaves is a constant for the specific type of atom—allowing for a universal, standard measure of time.

In February of 2022, physicists from the University of Wisconsin-Madison made one of the highest-performing atomic clocks ever. These clocks can measure differences in time with an error of only one second every 300 billion years. The physicists also created the first "multiplexed" optical clock, which is where six different clocks exist in the same setting. To achieve this, they separated strontium atoms into multiple clocks arranged in a line in the same vacuum chamber. This positioning allowed them to run meaningful experiments for much longer than their laser would allow in a normal optical clock. This breakthrough will allow scientists to search for gravitational waves and even attempt to detect dark matter.

Later in July 2022, a research team from Birmingham University developed next-generation atomic clocks that not only have a significant reduction in their typical size, but are also now strong enough to be transported out of the laboratory and utilized in the real world. Usually, atomic clocks are around 1,500 liters, butthese next-generation clocks are only around 120 liters. The newly developed clocks are about 10,000 times more accurate than the standard optical atomic clocks. In areas such as global trading in stocks and online communications, where fractions of a second make a huge difference, these redefined clocks will have a huge impact.

As researchers continue to make major strides in the advancement of atomic clocks, they open up the possibility of redefining the standard unit (SI) of measurement. These new models will allow scientists to perform experiments around mysterious concepts such as dark matter and dark energy, thereby gaining a better understanding of whether our physics fundamentals are constant or if they change with time. These seemingly simple clocks have the possibility of unlocking a better understanding of our world and improving the systems we have implemented within it.

REFERENCES:

Nelson, Jon. "What Is an Atomic Clock?" NASA. NASA, June 19, 2019. https://www.nasa.gov/feature/jpl/what-is-an-atomic-clock.

"Ultraprecise Atomic Clock Poised for New Physics Discoveries." ScienceDaily. ScienceDaily, February 16, 2022. https://www.sciencedaily.com/releases/2022/02/220216112210.htm.

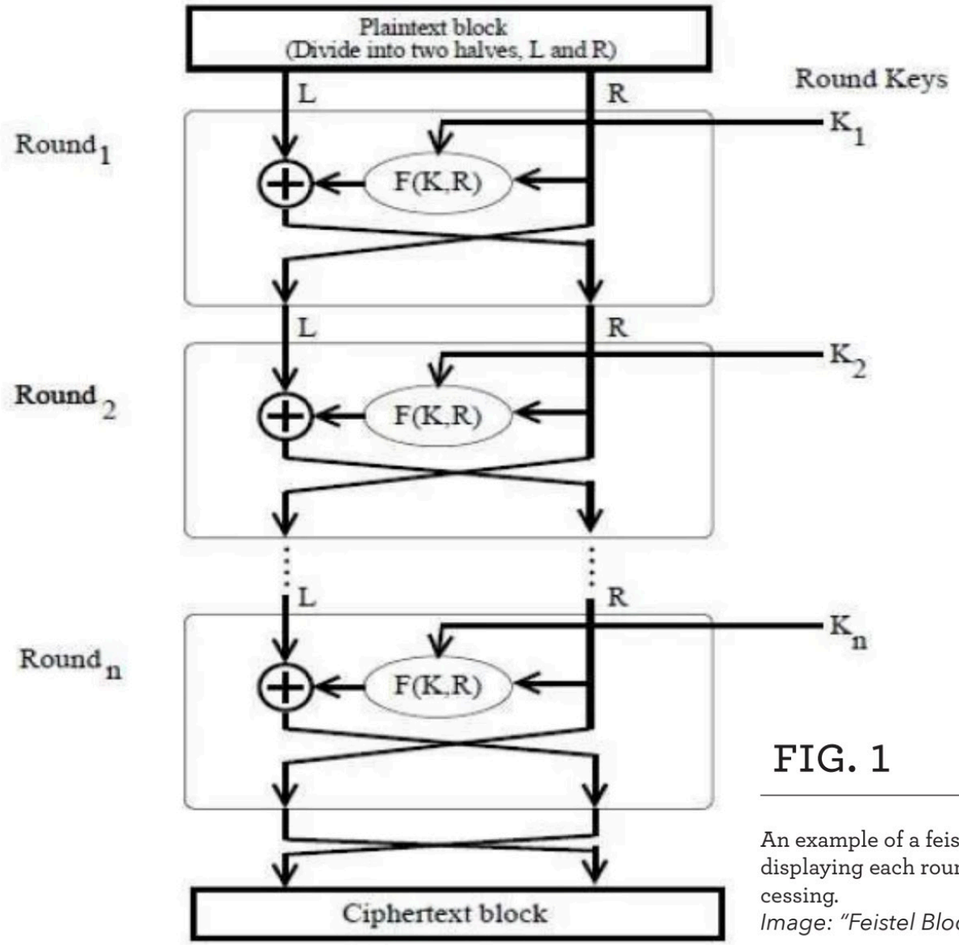


FIG. 1

An example of a feistel cipher, displaying each round of processing.
Image: "Feistel Block Cipher."

FEISTEL CIPHERS & SYMMETRIC KEY ENCRYPTION

Protecting Your Data without the Computational Stress

VICTOR ROBILA

Every transaction, search, and text you send is encrypted. The days of unencrypted bank transfers and messages have long passed as we take more steps to protect ourselves against ever-present cyber threats. Even just from browsing the news, you may have heard terms such as "public key," and "asymmetric encryption." These new developments in encryption have rapidly gained popularity, but it's necessary to see if current methods are the best.

Asymmetric key encryption, known for using pairs of public and private keys to encrypt and decrypt data, is known for heavy CPU usage and taking a toll on networks due to large data size. As more applications are found for this encryption, these problems only grow, even if optimizations are made. An older form of encryption, symmetric key encryption, and a specific form of symmetric key encryption, Feistel ciphers, can offer a solution to this pressing issue.

Symmetric key encryption is symmetric, using just one secret key to both encrypt and decrypt data. The key is exchanged between the two parties exchanging data. For example, you would exchange the key with the bank in which you are making a deposit or a withdrawal. The benefits come from using only one key, as only that piece of information needs to be transferred.

Feistel ciphers are a specific type of symmetric key encryption that have applications in various places. The cipher starts with plaintext, such as a text message. The block is divided into two halves, a left and a right half. There are several rounds of processing for this plaintext, each having a substitution and a permutation step. In Figure 1, a function with keys K1, K2, K3… transforms the right part of the plaintext which is then split again and the process repeats. The repeatability and ability to continually add rounds are two of the Feistel cipher's main benefits and show that old methods can be continually applied today to resolve problems in existing infrastructure.

REFERENCES

"Feistel Block Cipher." Tutorials Point. Accessed January 2, 2023. https://www.tutorialspoint.com/cryptography/feistel_block_cipher.htm.

"Feistel Cipher." GeeksforGeeks, February 24, 2022. https://www.geeksforgeeks.org/feistel-cipher/.

Hare, Valerie. "What Is a Feistel Cipher?" tokenex, October 10, 2022. https://tokenex.com/blog/vh-what-is-a-feistel-cipher/.

Peter Smirnoff & Dawn M. Turner (guests). "Symmetric Key Encryption - Why, Where and How It's Used in Banking." Cryptomathic. Accessed January 2, 2023. https://www.cryptomathic.com/news-events/blog/symmetric-key-encryption-why-where-and-how-its-used-in-banking.

4. Topics in Theoretical Computer Science

BUT WHAT EXACTLY IS A BIT?

ETHAN UPPAL

SIn 1948, Claude Shannon published his seminal paper, A Mathematical Theory of Communication. In it, he initiated information theory, the field of mathematics concerning the quantification and transmission of information, by systematically developing notions of communication and entropy. Information, however, is hard to define. Most people have a vague understanding of what this word means, but to fully comprehend this elusive concept, let's look at an example. The most straightforward source of information is a coin flip: its result is either head or tails. One way to approach the information contained in a coin flip is to ask how many yes-or-no (binary) questions you need to determine the flip. For coins, it is trivial: a single question will do. Thus, we can say that a coin flip contains one bit of information. In other words, we only need to ask one binary question to know the entirety of the flip. What about two coin flips? We need to ask two questions, so the information in two coin flips is two bits. In general, n coin flips have n bits. Let's compare the relationship between the number of bits and the number of distinct possibilities they express. One coin flip has two outcomes; two coins have four. In general, n coin flips have 2n possible results. Information is a measure of uncertainty.

A single fair coin is a simple case, but most real-world phenomena have many more sources of uncertainty in different probability proportions. Let's investigate a more complex scenario where we have a biased coin with a 1/3 chance of heads and a 2/3 chance of tails. How much information does one flip of this coin contain? It's not entirely obvious what binary questions we must ask to determine the flip's result, so let's attack this problem in reverse. If we flip the coin three times, we expect one to be heads and the other two to be tails. If n coin flips have 2n results, p results imply log2(p) flips–this is the definition of the logarithm. Using logarithm laws to manipulate that equation, we derive that p results also equals -log2(1/p). The information from one of the sides is the number of flips times the frequency of that flip, so if we add sides, we get the total: -1/3log2(1/3 - 2/3 log2(2/3), which is around 0.91. It makes sense that a rigged coin contains less information than a fair coin because you already know a little about the result, i.e., that it is more likely to be tails.

We write the general expression for information as H=-inpilog2(pi). The letter H is used because of how the quantity relates to an earlier one, Maxwell's entropy. Indeed, we can apply this formula to a physical system as much as we can to computers. Treating nature as Turing-complete has ramifications beyond this formula because it enables, for example, programmable matter in quantum physics. Note that the choice of a base-2 logarithm is arbitrary, and a different base leads to a different unit in place of the bit. Often, base-10 units are used when performing Bayesian analysis to determine the strength of the odds ratio in inference. Claude Shannon did not realize how fundamental and widely applicable the concepts he laid out in the paper would become, but he later changed the name from "A Mathematical Theory of Communication" to "The Mathematical Theory of Communication" to reflect the immense importance his work had in leading humanity into the information age.

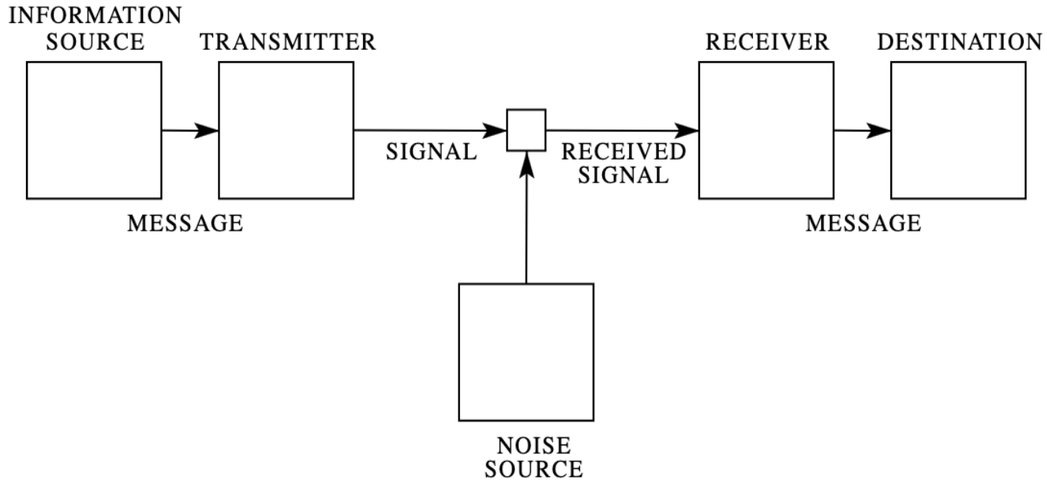


FIG. 1

caption

Image: The Bell System Technical Journal

REFERENCES

Claude E. Shannon. "A Mathematical Theory of Communication." Reprinted with corrections from The Bell System Technical Journal, Vol. 27, pp. 379–423, 623–656, July, October, 1948. https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf.

THE K-NEAREST NEIGHBORS ALGORITHM

AMY MA

If you wanted to recommend a movie to a stranger, how would you do it? You'd likely want to know what movies they have watched in the past and maybe what types of movies their friends watch. The inference you are making is an example of a k-nearest neighbors algorithm. The algorithm is based on the principle that people are likely to make the same decisions as others with similar profiles.

The k-nearest neighbors (k-NN) algorithm is a supervised learning algorithm, meaning that given a training dataset consisting of some points sorted into categories, it makes a prediction about the category of other points. The k-NN algorithm makes a prediction about one point based on the k closest points to it. Closeness is used to measure similarity. Between two points it may be determined in terms of Euclidean distance or by how many edges link the two points together on a graph. For example, a 1-NN algorithm would classify a point as the same category as the nearest point, so it would classify the green point in Figure 1 as blue. When k is greater than 1, the algorithm classifies a new point as the category that the majority of the k closest points are in, so a 3-NN algorithm would classify the green point as red because two out of the three closest points are red.

The k-NN algorithm is often used for recommendations. For example, YouTube will recommend videos you might like based on which videos you have watched in the past and what videos others like you have watched. K-NN algorithms can also be used for image recognition: by comparing an unknown image to ones in a database, the algorithm will identify and name objects based on the k nearest images. Although real recommendation or image recognition algorithms will often be more complex than k-NN, they are often still based on the same principles, making k-NN a powerful concept.

REFERENCES

"What Is the K-Nearest Neighbors Algorithm?" IBM. Accessed Jan 20, 2023. https://www.ibm.com/topics/knn.

Harrison, Onel. "Machine Learning Basics with the K-Nearest Neighbors Algorithm." Medium. Towards Data Science, July 14, 2019. https://towardsdatascience.com/machine-learning-basics-with-the-k-nearest-neighbors-algorithm-6a6e71d01761.

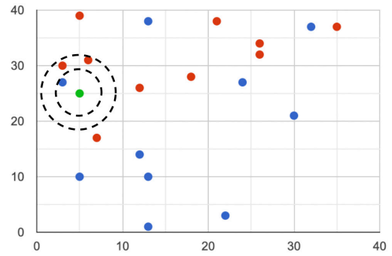


FIG. 1
Image: Amy Ma

RANDOMNESS IN CODE

KAYA PARIKH

Computers require very specific information to successfully determine the sequence of 1s and 0s they need to function. This makes creating truly random, roll-of-the-dice style programs extremely difficult. Random data must be obtained in such a way that is specific enough for computers to understand and use, but also still keeps its intrinsic ability to randomly produce one of a set of outputs. The programmed actions to get this data for uniform randomness (i.e. providing an equal chance for all outputs) can be separated into two categories: physical device-based random generators and pseudo-random generators, which are based on algebraic functions. Physical device-based random generators are fed information from physical readers which are connected to external items that possess constantly changing numbers, such as time, or a radioactive atomic decay source, which produces an unpredictable number for the time between particle detections. However, these types of random generators are often costly, clunky (especially with the particle detection tubes!), and inefficient.

Pseudo-random number generators, on the other hand, have the potential to generate more random numbers without the same dependency on outside-world behavior. Algorithms commonly define elements of a certain random set and provide examples of outputs given a function of the elements. However, the majority of these still use some basic element of randomness from the external environment to create a smaller random data set that can be built upon. When this is not included, the generator faces the risk of being "discovered" by users, a serious problem for lottery-based programming for businesses dependent on unsuccessful attempts to win money and prizes.

Though neither extremes are considered completely random, over the past decades humans have come closer to more truly uniform random generators with a confluence of the two unique techniques, overall providing better stability for our online activity.

REFERENCES

L'Ecuyer, Pierre. "History of Uniform Random Number Generation." Proceedings of the 2017 Winter Simulation Conference, December 3, 2017: 202-230. https://www.informs-sim.org/wsc17papers/includes/files/016.pdf.

THE LEFTOVER HASH LEMMA

How does online security work?

SAM HUANG

Cryptography is an incredibly important field in our modern lives. Without it, we would constantly be subject to people stealing our information and using it for nefarious purposes, such as hacking our bank accounts, blackmailing, and replacing all the files in your Google Drive with CollegeBoard videos. It's not only important to understand the complexity of cryptography, but also fun! We'll be delving a bit deeper into cryptography by focusing specifically on the leftover hash lemma, an important mathematical tool in cryptography.

A bit is the most basic way of storing information in computers: it is either 0 or 1. By stringing many bits together, we can transmit complex information. Let's say that Alice has a secret key that consists of n bits (title drop). However, Bob, her nemesis, has managed to figure out some number m of the bits, where m < n. Bob doesn't know all the bits, so there's still some hope left. If Alice wants to create a new secret key, she'll obviously want to create one using the bits that Bob doesn't know. Unfortunately, Alice has no idea which bits Bob knows, just that he knows m out of n total bits. How can Alice navigate this situation?

As it turns out, the leftover hash lemma states that Alice can always produce a new key of about n-m bits, of which Bob has "almost no" knowledge. The term "almost" in mathematics is complicated, but here it means that the knowledge Bob has tends to zero: he might as well know nothing about this new secret key. Therefore, if Bob knows m bits, we can create a new key with about n-m bits that almost perfectly matches the bits Bob doesn't know, without even knowing which bits Bob knows! Isn't that neat?

So, how does any of this work? Let's get into the mathematical side: specifically, we want to deal with probability theory. Let us consider a random variable N. In probability theory, a random variable is a function that maps possible outcomes to a measure space. A function is a mathematical object that has an input and an output. For example, when 4 is inputted into the function f(x) = x2, the corresponding output will be 42, which is 16. However, functions are not just limited to real numbers: we can have functions of any set to any other set. To give a concrete example of what was explained earlier, let's consider a coin flip. Let the random variable (which is a function) map from the set {Heads, Tails} to {1,-1}, where N(Heads) = 1 and N(Tails) = -1. For our more experienced readers, we can say that N is a function with domain {Heads, Tails} and codomain {1,-1}, which may be expressed succinctly as N : {Heads, Tails} -> {1, -1}. The entropy of a random variable N is written as H(N), defined as E[-log(p(N))] (the choice of log varies, but log2 uses bits as units), where E[f(x)] is the expected value of a function f(x): that is, it is the weighted average of all possible values, weighted using their probabilities. p(N) is a probability function that maps the outputs of N to the set {0,1}. Entropy is essentially how unpredictable the random variable is: the higher the entropy is, the more chaotic and uncertain the result of the random variable is. Using the idea of entropy, we may derive minimum entropy, which is the entropy calculated from the most likely outcome rather than the average of all the possible outcomes. The leftover hash lemma states that it is possible to extract a length of n-m bits such that it has almost minimum entropy, and that the bits are almost uniformly distributed. Bob will have very little knowledge of the new string of n-m bits because the bits we choose for our new secret are uniformly distributed across the original n bits. The minimum entropy of the bits guarantees that we are choosing the bits for our new string as uniformly random as possible. Say, for example, that Alice has a key 101011101 with length 9 and Bob knows 4 bits, 1010. The leftover hash lemma states that it is possible to create a new key of length 5 where Bob knows a vanishingly small part of the key; Alice can create a new key 01101 that only has the first 0 as one of the bits Bob knows, uniformly choosing the bits from the original key. This is a tiny example, and the lemma is much more effective when considering keys with hundreds of bits, where Bob will be hopeless to crack the new key.

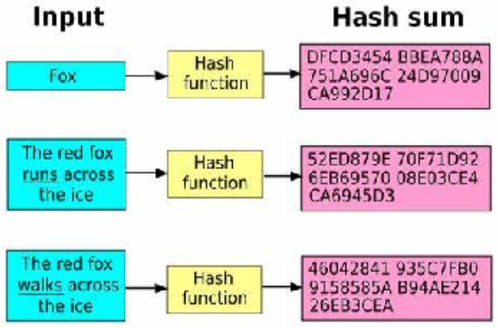


Fig. 1

A hash function maps bits in an input to an output that is difficult to reverse.

This article was in no way comprehensive, and only covers the basics of the leftover hash lemma. However, it shows the deep computational complexity of cryptography systems, and an opportunity to appreciate the world of mathematics happening behind our business transactions, emails, and cat videos.

SOURCES

Impagliazzo, Russell; Levin, Leonid A.; Luby, Michael, Pseudo-random Generation from one-way functions, in Johnson, David S. (ed.), Proceedings of the 21st Annual ACM Symposium on Theory of Computing, May 14-17, 1989, Seattle, Washington, USA, {ACM}, pp. 12-24, doi:10.1145/73007.73009, S2CID 18587852

Blum, M., and Mica li, S., How to Generate Cryptographically Strong Sequences of Pseudo- Random Bits, SIAM J. or~ Computing, Vol. 13, 1084, pp. 850-864, FOCS 1082

Rubinfeld, Ronnit; Drucker, Andy (April 30, 2008), Lecture 22: The Leftover Hash Lemma and Explicit Extractions, Lecture notes for MIT course 6.842, Randomness and Computation, MIT

Tsurumaru T. Leftover Hashing From Quantum Error Correction: Unifying the Two Approaches to the Security Proof of Quantum Key Distribution. IEEE Transactions on Information Theory. 10.1109/TIT.2020.2969656. 66:6. (3465-3484).

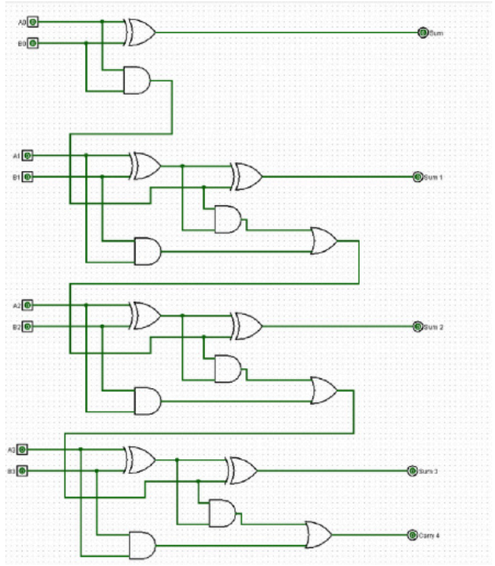
BINARY ADDITION WITH LOGIC GATES

EDEN REINFURT

When you use a calculator, do you ever wonder how it is able to perform addition?

In digital electronics, addition is usually performed using logic gates. Logic gates are the basic building blocks of digital circuits and most electronic devices have some sort of logic gate in them. They are used to implement binary logic functions, such as AND, OR, NOT, NAND, NOR, and XOR. A logic gate takes in one or more binary inputs, 0, representing false, and 1 representing true, and returns a single output. For example, the AND gate, which only outputs true if both inputs are true, takes two binary inputs, each either 0 or 1 and only outputs a 1 if both inputs are 1s. The OR gate, on the other hand, outputs a 1 if either of the inputs is a 1; otherwise it outputs a 0.

These simple logic gates are able to come together to carry out much more complex calculations. The most basic of these is addition. Binary addition involves half adder and full adder circuits. A half adder performs the basic addition of two binary digits and generates two binary digits, a sum bit and a carry bit. The sum bit is the ones place in the addition, while the carry bit is the twos place, which is carried over to the next column of the addition if the digits add up to greater than 1. It is made up of an XOR gate and an AND gate. The XOR gate, short for exclusive-or gate, meaning that exactly one of the inputs has to be true for it to output a true. It takes in two inputs from the same place value in the two binary numbers being added, and outputs a 1 only when it receives a 0 and a 1. When it receives two 0s or two 1s, it outputs a 0. The AND gate is used to figure out if a 1 must be carried over into the next column, since that will only be the case if two 1s are inputted. The half adder determines the ones place for the final output, coming from the sum bit, since if a 0 and a 1 are added, the final result is a 1, but if two 1s are inputted, it outputs a 0 and a 1 is carried over to the next column. In figure 2, the first two logic gates form the half adder, with the XOR gate on top, and the AND gate below it.



A full adder uses the structure of a half adder but extends this functionality to handle the carry-in bit from a previous addition, allowing it to perform the addition of more than two binary digits. It is essentially two half adders added together, with the second half adder dealing with the carry bit and the sum bit from the first half adder. In addition, it has an OR gate, which combines the results of the two AND gates to determine if a 1 will be carried over into the next column. Multiple full adders can be cascaded together to perform the binary addition of larger numbers, with each full adder performing the addition of one bit and generating a carry bit for the next full adder in the chain. Each of the sum bits gives a binary digit for that place value, and the final carry bit becomes the binary digit for the greatest place value.

For example, take the addition of 2 and 3, 10 and 11 in binary. First, a half adder would be used to add the ones places, which are 0 and 1. These would be the inputs for both the XOR gate, which would output a 1, and the AND gate, which would output a 0. That means that the ones place for the addition would be a 1, and the carry bit would be 0. Next, the twos place for both numbers would be inputted into a full adder, along with the carry bit. The first XOR gate would output a 0, since it receives two 1s which cancel out, while the first AND gate would output a 1. The second XOR and AND gates would receive the output of the XOR gate and the carry bit from the first half adder, and both output a 0 since both inputs are 0s. That means that the twos place is a 0, since it is given by the output of the second XOR gate in a full adder. Finally, the outputs from the two AND gates would be inputted into the OR gate, to output a 1. Therefore the final output would be 101, which is 5.

Because of the simplicity of logic gates and adders, they can be applied to more than just digital electronics. Using these principles, people have created calculators out of cardboard, legos, wood, marbles, dominoes, blocks in minecraft, and much more. Essentially, what is required to perform binary addition is the combination of two binary inputs plus a carry-in to generate an output and a carry bit, which is done very simply through these logic gates.

Fig. 1

Logic gates for an 8-bit binary calculator.

REFERENCES

101 Computing. “Binary Additions Using Logic Gates.” Last modified January 4, 2018. https://www.101 computing.net/binary-additions-using-logic-gates/.

Electronics Tutorials. “Binary Adder and Binary Addition Using XOR Gates.” Accessed May 18, 2023. https://www.electronics-tutorials.ws/combination/comb_7.html.

TechTarget. “Logic Gate (AND, OR, XOR, NOT, NAND, NOR and XNOR).” Last modified December 2020. https://www.techtarget.com/whatis/definition/logic-gate-AND-OR-XOR-NOT-NAND- NOR-and-XNOR.

LONGEST INCREASING SUBSEQUENCE

CHLOE ZHOU

Let's take a look at a classic algorithm problem: how to find the longest increasing subsequence of an array. To start this problem off, we have to define a subsequence. If we remove some numbers from an array, we get a subsequence of the array. For example, [4, 8, 9] is a subsequence of [4, 10, 4, 3, 8, 9]. If the numbers in the subsequence are in strictly increasing order, the subsequence is an increasing subsequence. Now that we know what the problem is, how do we find the longest increasing subsequence (LIS) in an array?

One might first think to solve this by checking all 2n subsequences of the array of length n, and then find the longest increasing ones (there can be more than one LIS). Checking each subsequence takes a time proportional to n, or O(n) in big O notation – a theoretical measure of the time-efficiency of an algorithm – so this algorithm has a runtime of O(n x 2n). The algorithm is very inefficient because the short subsequences are parts of the longer ones, and we have performed many repetitive computations.

To avoid this repetition, we can solve this problem recursively, and save the partial results along the way to be used in later steps. If we call the first k numbers of an array the k-prefix of the array, then there are n such prefixes in the array (1-prefix, 2-prefix, …, n-prefix), where each prefix is contained by the larger prefix after it. Let's also call the LIS that ends at the last number of the k-prefix LISk. If we store the lengths of all LISi for i < k, then we can use them to find LISk, because LISk could be formed by adding the kth number to a previous LISi – this is the source of our recursion, which saves a lot of expensive computation. Due to the definition of LISi and by making use of our cache, we can do comparisons between all LISi to find the longest one for our overall LIS. Finding a LISi has O(n) runtime, while going through each prefix is also O(n). Therefore, this algorithm has a polynomial runtime of O(n2), much faster than the exponential runtime of the naïve solution. This is a great improvement in efficiency!

There actually exists an algorithm that has a further optimized runtime, based on a card game called Patience. We can consider the numbers in our array as an ordered deck of cards. The first card is placed down. For each successive card, place it in the leftmost pile whose top card is greater than the new card. If no such pile exists, place the card in a new pile. At any stage during this algorithm, the number of piles equals the length of the LIS so far. To find the position to insert each of the n cards, we use a binary search – an efficient algorithm for finding an item in a sorted list – which takes O(log(n)) time, so the total runtime is O(n x log(n)), even better than the previous algorithm! This is sometimes called a greedy algorithm order to reach the global optimum, but it doesn't exist for every problem.

The problem of finding the LIS of an array actually has applications in many fields, including aligning organisms' genomes. Alignments are a powerful way to find new information about the DNA aligned, such as shared evolutionary history, or common structural function. Because genomes are billions of base pairs long, it is important to have an efficient algorithm for doing so – and hopefully this article has shown the logic behind three methods to do this very task!

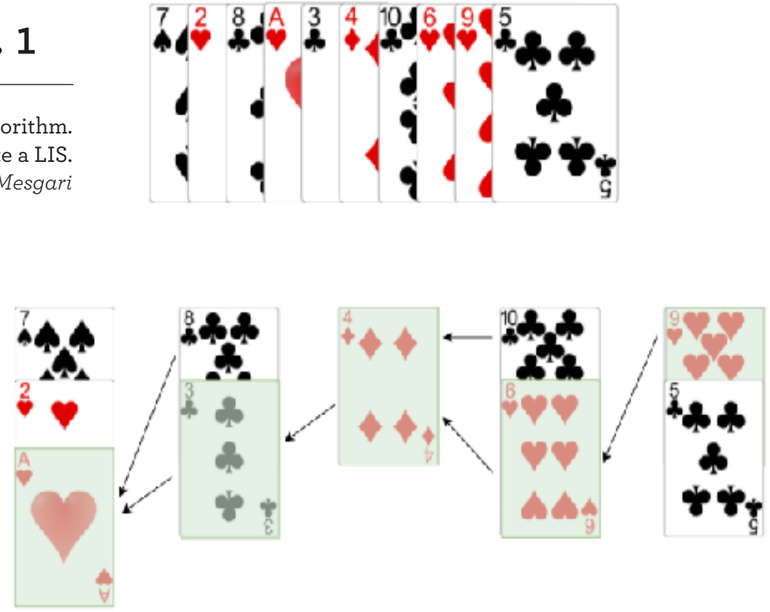
REFERENCES

Mesgari, Payam. 2021. "Part 2: The World of Subsequences, Longest Increasing Subsequence." Last modified July 24, 2021. https://www.techjournal.nl/2021/07/24/part-2-the-world-of-subsequences-longest-increasing-subsequence/.

Princeton University. n.d. "Longest Increasing Subsequence." Accessed January 21, 2023. https://www.cs.princeton.edu/courses/archive/spring13/cos423/lectures/LongestIncreasingSubsequence.pdf.

Fig. 1

A patience sorting algorithm. The links indicate a LIS.
Image: Payam Mesgari



5. Technicalities, Mechanics, and Tidbits

AI IMAGE UPSCALING

SIMON ESKIN

Machine learning has scared people for decades, and it's finally here. In some ways, it has lived up to fears that it will become sentient. Programs like ChatGPT, DALL-E, and StableDiffusion can almost simulate human creativity, and deepfakes of politicians could threaten the integrity of the democratic process. Thankfully, machine learning isn't always so sinister. One relatively harmless technology that has been improved by machine learning networks is image upscaling: increasing the resolution of low-quality images.

Traditional image upscaling techniques rely on interpolation, which uses the color values of each pixel in a low resolution image to determine what the spaces in between the pixels look like. The most basic types of interpolation, including nearest neighbor interpolation, linear interpolation, and cubic interpolation, assume some relationship between neighboring pixels. Nearest neighbor interpolation is the simplest type of interpolation, where the spaces in between pixels are assumed to be the same color as the nearest pixel. This method rarely is able to add significant amounts of detail to images and results in upscaled images having blocky edges because there is no gradient between the source pixels. Linear interpolation assumes there is a linear progression between the RGB values of neighboring pixels, cubic interpolation assumes a cubic progression, and so on and so forth. As the interpolation technique becomes more complex, the upscaled image starts to look more realistic, but takes longer to compute.

Interpolation can be an effective method to increase the resolution of an image, but higher levels of interpolation can be very taxing on hardware. Another downside of interpolation is that it can create digital artifacts, which are little patches of pixels where the algorithm finds details in places where the source image does not have any. In recent years, another way to upscale images has emerged: AI upscaling. Instead of calculating gradients between pixels, AI upscalers are trained to know what certain types of images are supposed to look like. These upscalers have been trained using millions of different images, and they know how certain objects or landscapes are supposed to look. Given a low quality image of a tree, an AI upscaler can recognize the tree and create believable branches whereas interpolation might have trouble differentiating between each branch in the low quality image. AI upscaling uses neural networks to these realistic, high resolution images without creating the digital artifacts that interpolation techniques often do.

AI upscaling creates more realistic images and fewer digital artifacts than interpolation, and requires less computing power to run. It can be applied to images, videos, and even video games. Nvidia's DLSS (Deep Learning Super Sampling) uses AI upscaling to improve the performance of video games without degrading the image quality. DLSS shrinks the resolution and then upscales the smaller image to the original resolution. This method allows the computer to run a much less taxing version of the game (at a low resolution) without losing any visual quality. DLSS reduces power consumption without changing the quality of the game, making it environmentally friendly in addition to its performance improvements.

Overall, AI image upscaling is a very promising new way to enhance old images and videos. It consumes less computing power than interpolation and still manages to increase the accuracy of the upscaled images. Since AI upscaling is such a novel technology, it will only get better in the future. Maybe we'll be able to upscale like they do in CSI: "Enhance!"

FIG. 1

Image: Gigapixel AI

REFERENCES

Citations:

"Overview of Interpolation Modes." Intel, Intel, https://www.intel.com/content/www/us/en/develop/documentation/ipp-dev-reference/top/volume-2-image-processing/ipp-ref-interpolation-in-image-geometry-transform/overview-of-interpolation-modes.html.

Miklós, Póth. "Image Interpolation Techniques - California Institute of Technology." IMAGE INTERPOLATION TECHNIQUES, California Institute of Technology, https://web.ipac.caltech.edu/staff/fmasci/home/astro_refs/InterpMethods.pdf.

Gigapixel AI, Topaz Labs, https://www.topazlabs.com/gigapixel-ai.

"Nvidia DLSS Technology." NVIDIA, NVIDIA, https://www.nvidia.com/en-us/geforce/technologies/dlss/.

HOW TO

Make Your Website More Accessible for Visually Impaired People

ALEXANDRA BERNSTEIN

I The internet has changed the world of research to an incredible extent in the last twenty-odd years. Within a tenth of a second after pressing "enter" on your keyboard, any query can be answered with millions of results. Websites are invaluable in our modern-day society, yet a surprisingly small number of them have made efforts to tailor to the needs of blind and visually impaired people. Small, faint text, images without text descriptions, complex layouts, and many other elements of typical websites make it difficult for visually impaired people to navigate the internet and locate information. However, this issue can easily be resolved if website creators do a few simple things to adjust their website designs.

Having as much text as possible is one of the most important parts of making a website accessible since many visually impaired people have software that can read out the text for them. In-depth descriptions of images, charts, and graphics allow the website user to access quantitative and qualitative information that they may need to understand the topic of their research. For people who are not blind, but have other visual impairments, incorporating color contrast between the text or images and the background allows them to see and read the descriptions more clearly.

Another element of website design is that the creator can label the headings of each section in the HTML code of the website so that the website user's audio software can more easily identify the "breaks" on a website page that non-visually impaired people usually recognize in paragraphs. When the headings are included in the HTML code, the website's search engine optimization (SEO) is improved, meaning that it will come up sooner as a website when a search engine answers a question. This allows visually impaired people to find high-quality information more easily. Including "alt text" as textual descriptions of the images on the website also improves the SEO of the website. For all website design, regardless of targeting an audience of visually impaired people, SEO is important for increasing viewer traffic, so adding headings can help website creators.

A third component of website design is making the language of the text clear so blind or visually impaired people can adjust the language on their audio software that reads the text aloud to them. Identifying the language in the HTML code, with the coun-

FIG. 1

This cartoon exemplifies the audio software that many visually impaired people use to navigate websites. The importance of enlarged text size is also shown.
Image: Pixelplex

try if the language is spoken in more than one place, can enable the audio software to navigate the website and translate text into a different language if necessary. Even switching from British English to American English is important to users who may be unfamiliar with British English idiosyncrasies. An example of what language identification in the code for British English looks like is: <html lang="en-GB">

These are only a few examples of some of the ways website creators can develop inclusive, accessible websites, but even including one or two allows visually impaired people to access information more easily. Even for non-visually impaired people, having things like high contrast and larger or more apparent headlines can make it easier to identify key information, especially when our eyes become strained after hours of looking at a computer screen. Being able to rest your eyes from squinting at tiny text and faint images is something that we can all benefit from.

REFERENCES

Koorevaar, Danielle Batista. "Make Your Website Accessible for the Blind and Visually Impaired." Trusted Shops, April 26, 2021. https://business.trustedshops.com/blog/make-website-accessible-for-blind-and-visually-impaired.

LOOKING BACKWARDS, MOVING FORWARDS

IAN CHO

It is a moderately well-known fact that Microsoft Excel incorrectly counts the year 1900 as a leap-year. And though I'm sure that this little tidbit will help all of the numerous spreadsheet users out there, that's not quite what this article is about. The reason for this peculiar bug, as well as why it hasn't been corrected yet, dates back to the ancient times of 1985, when a software known as Lotus 1-2-3 was the leading spreadsheet software. When Microsoft was creating Excel as a competitor to Lotus, they presumably wanted to tap into Lotus' existing users by making porting data from Lotus to Excel as seamless as possible. As such, Microsoft purposefully implemented the same leap year error present in Lotus to make use of the same serial date system and maintain the two programs' compatibility.

But why keep the bug now, even as Lotus 1-2-3 has completely fizzled out? The reason lies in a concept known as backwards compatibility. Backwards compatibility is the concept that a newer version of a hardware or software should still be able to support an older version of a hardware or software; the extent to which this is required to be done depends on the approach the company in question uses. For example, the newer generation of Xboxes can run games from the original Xbox console, but a Playstation 5 can not natively run Playstation 1 games. But though the level to which backwards compatibility should be maintained is a point of debate—debaters asking to what point supporting older systems is reasonable—it is generally considered good design practice to maintain backwards compatibility as thoroughly as possible.

Thus, Microsoft purposefully maintains the irritating bug that was implemented years ago, because the drawbacks of breaking backwards compatibility heavily outweigh the benefits. The time to rip off the bandaid was in 1985, not now. If Microsoft were to fix the Excel bug today, it would break the countless number of spreadsheets that make use of the WEEKDAY function, among others. The damage that would be done to the data of various companies and firms is incalculable. In fact, Microsoft explicitly codifies the erroneous behavior as a requirement in its formal specifications for the OOXML (Office Open XML) file format, their patented format for representing spreadsheets. And though I'm sure that deliberately keeping a bug—especially one as trivially infuriating as that—torments every developer working on the program, vanquishing the erroneous leap year would give rise to a whole host of much larger issues.

FIG. 1

Image: Reddit

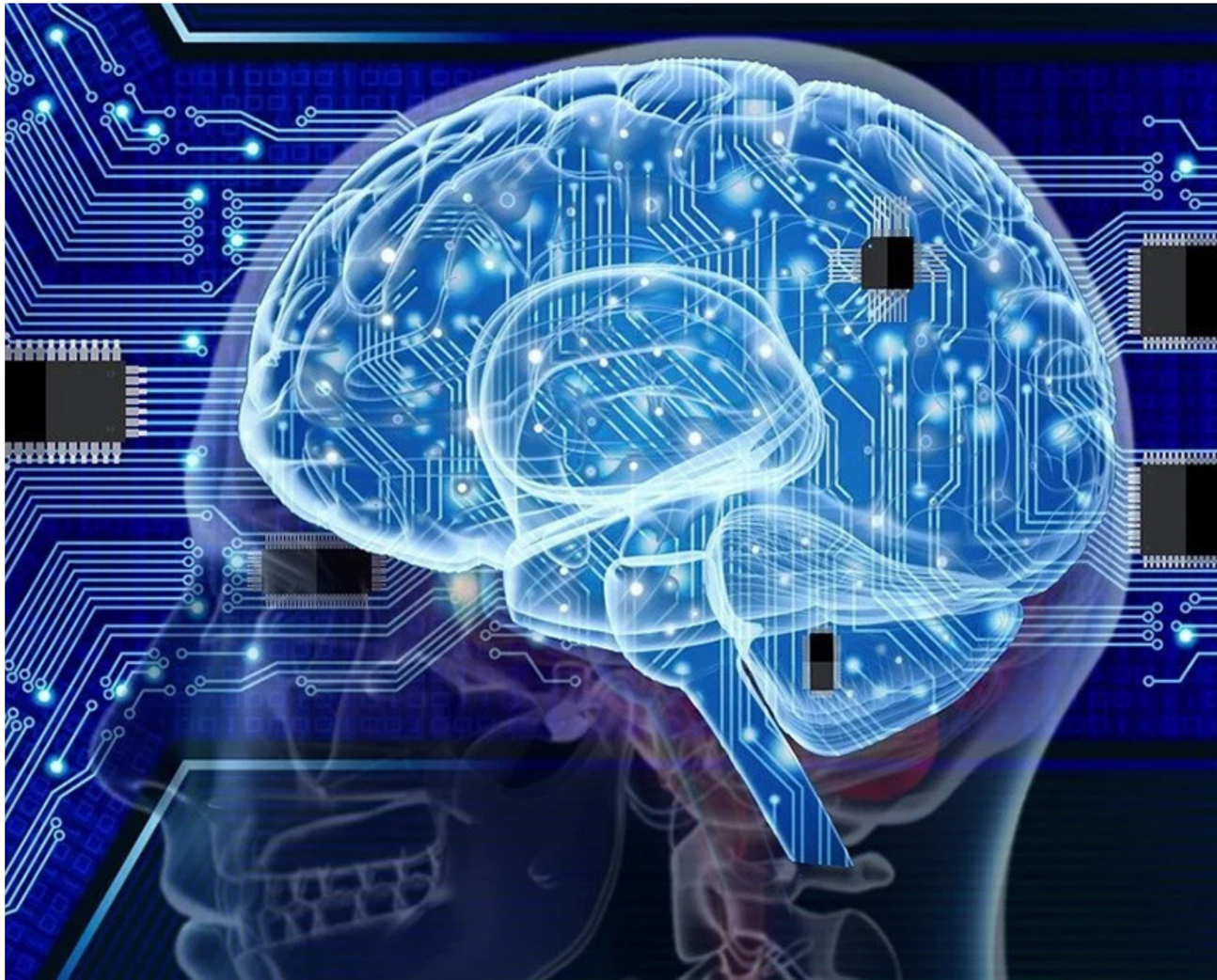
REFERENCES

Helenclu. “Excel Incorrectly Assumes That the Year 1900 Is a Leap Year - Office.” Office | Microsoft Learn. Accessed May 4, 2023. https://learn.microsoft.com/en-us/office/troubleshoot/excel/wrongly-assumes-1900-is-leap-year#:~:text=This%20assumption%20allowed%20Microsoft%20Multiplan,one%20program%20to%20the%20other.

Heshitha, Arunalu. “Is the PS4 Backwards Compatible?” Game Freaks 365, February 19, 2023. https://gamefreaks365.com/is-the-ps4-backwards-compatible/#:~:text=For%20example%2C%20if%20the%20PlayStation,model%20included%20PS2%20hardware%20inside!

Xbox Support. Accessed May 4, 2023. https://support.xbox.com/en-US/help/games-apps/backward-compatibility/what-games-are-compatible-with-my-xbox#:~:text=If%20you%20previously%20bought%20a,Xbox%20Series%20X%7CS%20console.

FIG. 1 Artificial neural networks are programs based on the network of neurons that make up the human brain, so that computers can learn things and make decisions the way we do.



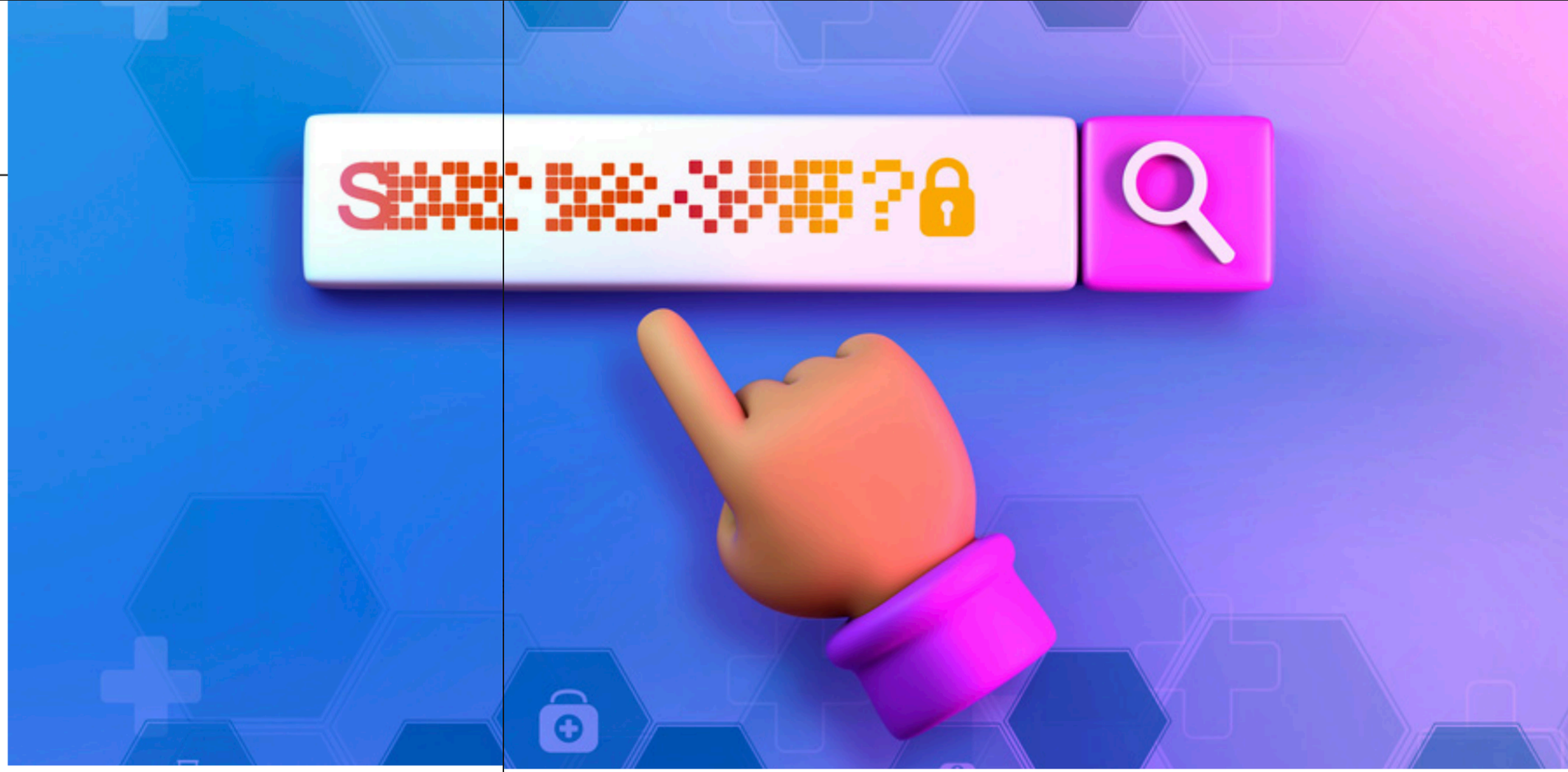
SIMPLEPIR

An Alternative to Google

ADDIS ADAM

Companies constantly use our internet activity to store information about us, though most people choose to ignore this unsettling truth. Simply searching on Google enables advertisers to learn more about us, using our own queries as tools to market more effectively. The answer seems simple: a secure, private way for us to surf the web without compromising our personal information. But, such a solution is easier said than done. For example, private information retrieval can often be much slower than public options. However, developing an efficient private data retrieval method is possible.

MIT researchers Alexandra Henzinger, Matthew M. Hong, Henry Corrigan-Gibbs and Vinod Vaikuntanathan, along with Google research scientist Sarah Meiklejohn, co-authored a paper presenting SimplePIR, their new method of private information retrieval. It is the fastest private information retrieval server ever created, though it comes with large communication costs. The team behind SimplePIR created a lower communication cost alternative: DoublePIR. SimplePIR requires users to download a 121 MB "hint" prior to making any queries, but DoublePIR's hint is only 16 MB. The tradeoff for a lower initial hint is lower throughput and higher communication required per query. In the future, the team hopes to improve upon SimplePIR and DoublePIR by reducing the communication and computation required.



REFERENCES

Zewe, Adam. "A Faster Way to Preserve Privacy Online." MIT News | Massachusetts Institute of Technology. Accessed January 30, 2023. https://news.mit.edu/2022/online-information-user-data-privacy-1207.

Henzinger, Alexandra, Matthew M. Hong, Henry Corrigan-Gibbs, Vinod Vaikuntanathan and Sarah Meiklejohn. "One Server for the Price of Two: Simple and Fast Single-Server Private Information Retrieval." Usenix. Accessed January 30, 2023. https://www.usenix.org/conference/usenixsecurity23/presentation/henzinger.

Olivares, Jose-Luis, MIT, and iStockphoto. SimplePIR. Accessed April 30, 2023. https://news.mit.edu/2022/online-information-user-data-privacy-1207.

FIG. 1

MIT Researchers have developed a novel method of private information retrieval that is 30 times faster than other methods. *Image: Olivares et al.*