COLLEGE OF ENGINEERING GUINDY
DEPARTMENT OF INFORMATION SCIENCE AND TECHNOLOGY
INFORMATION SCIENCE AND TECHNOLOGY ASSOCITION

InsTance

ISTA's OFFICIAL MONTHLY NEWSLETTER

ESTD. 2024

EDITION #00

OCTOBER 2024

PLACEMENT statistics. 43

Wells Fargo	4
Fidelity Investments	1
Citi Corp	6
Barclays	2
Oracle India	4
Infinera India	2
Société Générale	1
Athena Healthcare	1
SAP	2
Amazon	6
Trimble	2
KLA Tencor	1
Starten Systems	1
Apple India	2
Sagent M&C	1
Standard Chartered	1
Eucloid Data Solutions	2
Verizon India	4

Tech Trek 2.0 REPORT

SHANJANAA.G - 2021115099

Every Friday at 3:00pm, the Ada Lovelace Auditorium transforms into a launchpad for students ready to level up their skills at ISTA's very own TECH TREK 2.0!

The series has been a thrilling ride, packed with events that help students develop both professionally and personally. From refining interview techniques under expert guidance to unleashing creative marketing ideas that spark laughter and innovation, the sessions have been diverse and impactful. There's been plenty of mingling, with participants mastering the art of networking, minus the awkward staring phase, and some intense SQL-based challenges where budding data experts tested their skills.

Each event has been meticulously crafted by ISTA's different domains, ensuring a perfect blend of fun and learning. And the best part? TECH TREK 2.0 is still in full swing, with the Media and Industrial Relations Team just waiting to release participants into a creative spiral that no one saw coming.

As the series continues, the excitement builds, with everyone eyeing the grand prize—a ₹4000 prize pool that's up for grabs. With the final showdown on 14th October 2024 at the same place as always, anyone could take home the win. The clock is ticking, and the competition is fierce. Who will emerge victorious? Only time (and some serious skills) will tell!

An Introduction to the Adversarial attacks in the world of Computer Vision

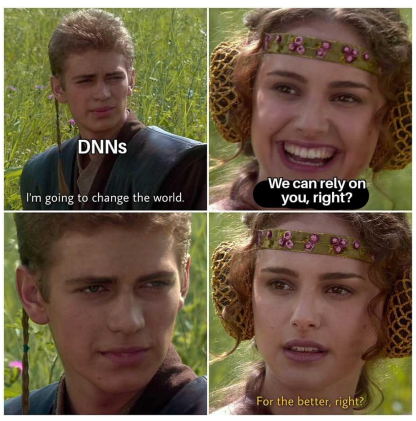
SALAI KOWSHIKAN - 2022115081

INTRODUCTION

Computer vision is one of the more exciting and rapidly evolving fields. It's an integral part of our daily life ranging between fun snapchat filters to critical security systems. A lot of systems depend on detecting objects with **Deep neural networks (or DNNs for short)** – from face recognition systems to autonomous driving cars.

Have you ever wondered that we are putting too much trust on these systems?

What if there was a consistent way to get past them?



Let me introduce you into the world of Adversarial Machine Learning. It all started at the MIT Spam conference in 2004, when John Graham-Cumming demonstrated the use of a machine learning model to generate spam that can get past the spam filter of another machine learning model by learning which words get flagged as spam through a trial-and-error method.

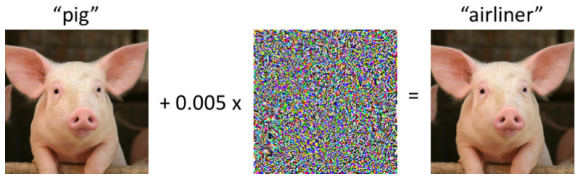
What he did is termed as an adversarial attack – It is a malicious attempt to fool the classification model. An adversarial attack is done by generating adversarial examples, which are perturbations to an input that results in incorrect classifications far from the truth.

As an attacker, the goal is to make a small perturbation in the input data to force a model misclassification. In some cases, these attacks can be targeted, meaning the input data is manipulated to resemble a specific class. However, adversarial attacks are often more effective when the perturbations aim to move the data away from its true class rather than into a particular one.

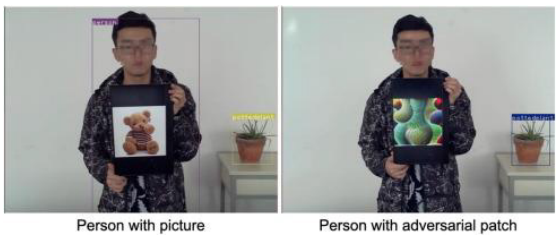
LET'S TAKE A TINY PEEK

Adversarial Attack can be classified in several ways. If the attacker has full knowledge about the model, it is known as a **white box attack**. On the other hand, when the attacker knows only about the inputs and their corresponding outputs, it is known as a **black box attack**.

A **Digital adversarial attack** is done by making modifications to the input image before it is fed into the classifier. Here is an example:



While digital attacks are highly successful and effective in tricking classifiers, they are near impossible to execute. Most models have well-structured pipelines that prevent any external interference with the input. This has led to the development of physical adversarial attacks, where perturbations are applied in the real world. A most famous example is the adversarial patch attacks, where a patch is pasted directly on the object, causing the model to misclassify it. Below is an example where the person flies under the radar by holding an adversarial patch.



Person with picture | Person with adversarial patch

WHO CAN SAVE US?

Robustness of a model is the metric used to measure the model's ability to withstand adversarial attacks. Improving a model's robustness is an active area of research. One such proposed method is to generate possible adversarial examples for the model and include them in the dataset.

The information presented here barely scratches the surface. It is a deep rabbit hole waiting to be explored.

For the interested readers, I highly encourage to dive deep on the latest research papers on the topic, some of which are cited below:

Amirkhani, A., Karimi, M.P. & Banitalebi Dehkordi, A. A survey on adversarial attacks and defenses for object detection and their applications in autonomous vehicles. Vis Comput 39,5293–5307(2023). https://doi.org/10.1007/s00371-022-02660-6

Naqvi, S.M.A., Shabaz, M., Khan, M.A. et al. Adversarial Attacks on Visual Objects Using the Fast Gradient Sign Method. J Grid Computing 21, 52 (2023). https://doi.org/10.1007/s10723-023-09684-9

S. Jain, "Adversarial Attack on Yolov5 for Traffic and Road Sign Detection," 2024 4th International Conference on Applied Artificial Intelligence (ICAPAI), Halden, Norway, 2024, pp. 1-5, doi: 10.1109/ICAPAI61893.2024.10541282.

Techtember Round Up

PURUSHOTHAMAN - 2022115109

TELEGRAM FOUNDER ARRESTED

Pavel Durov, the founder of Telegram, was arrested in France in connection with an investigation into crimes involving child pornography, drug trafficking, and fraudulent activities on the platform. French President Macron emphasized that the arrest was not politically motivated and that France remains committed to lawful free speech.

NEURALINK HUMAN TRIALS

Neuralink, Elon Musk's brain-computer interface company, has secured approval to begin its first human trials, recruiting people with paralysis. The trials have raised ethical concerns, and previous investigations were launched into animal mistreatment and biohazard handling by the company.

NETFLIX ANIME LEAKS

On August 6, pirated versions of anticipated anime series like the 'Ranma ½' reboot and 'Terminator Zero' leaked online through BitTorrent and 4chan, ahead of their official Netflix release, marking one of the worst leaks in anime history.

INTEL PATENT LAWSUIT

Intel was ordered to pay $2.18 billion to VLSI Technologies for infringing two processor patents. Intel is disputing the ruling, claiming the amount is excessive, given VLSI had not used the patents for over a decade.

EU vs WHATSAPP

Meta has introduced third-party chat integration in WhatsApp and Messenger to comply with the EU's Digital Markets Act. Users will now have the option to connect with third-party messaging apps, and features like reactions, direct replies, and read receipts will be available, with group calls and video calls expected by 2027.

SPOTIFY AI MUSIC SCAM

Michael Smith, a man from North Carolina, was arrested on September 4 for creating AI-generated music under fictitious band names and exploiting streaming services to earn over $10 million in royalties through fraudulent means.

GOOGLE MONOPOLY CASE

A U.S. federal judge ruled that Google has illegally maintained a monopoly in search and text advertising, violating the Sherman Act. This landmark case, filed in 2020, is the first major anti-monopoly ruling against a tech company in decades.

CHATGPT GAINS INTERNET BROWSING

OpenAI's ChatGPT can now search the web for current information, allowing select premium users to ask about real-time events. This update expands the AI's capabilities beyond its previous September 2021 knowledge cutoff.

INTERNSHIP statistics. 16

Wells Fargo	2
Fidelity Investments	7
Citi Corp	1
Barclays	5
Vegrow	1

The BINARY Puzzle

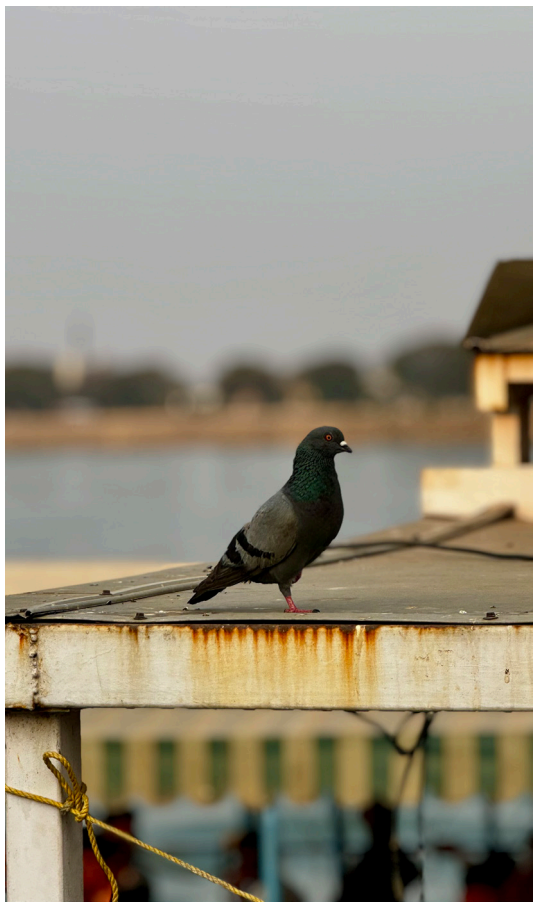
			0			1	
	1	1		0			
	1						1
		0					
						0	
1					0		
			0				
1				1		1	

RULES

1. Each box should contain either a zero or a one.
2. More than two equal numbers immediately next to or below each are not allowed.
3. Each row and each column should contain an equal number of zeros and ones.
4. Each row is unique and each column is unique. Thus, any row cannot be exactly equal to another row, and any column cannot be exactly equal to another column.

PHOTOGRAPHY corner.

RISHI KUMAR



2022115085

AJAY KUMAR

2022115086

I++ '24 SCOOP!

On October 25 and 26, the IST Department is set to host I++ 2024, the intra college symposium that's about to bring the entire campus together! Prepare yourself for a day filled with hands-on workshops and exciting tech and non-tech events that will challenge your skills, test your creativity, and offer plenty of fun along the way.

Whether you're here to dive deep into technology or just explore something new, I++ 2024 has something for everyone. And did we mention the cash prizes waiting to be won?

This is more than just an event—it's an experience. Dive into hours filled with innovation, intense competition, and invaluable learning, where every second matters. Don't miss the chance to be part of something unforgettable!

Stay tuned for more updates and mark your calendars—I++ 2024 is going to be legendary.

P.S. The winners of TECH TREK 2.0 will be awarded during the event, so make sure to be there!

See you there!
Yours,
ISTA