NORTH SOUTH UNIVERSITY

Department of Electrical & Computer Engineering

Research Article

Course Name: Engineering Economics and Management

Course Code: EEE452

DATA MISGUIDING AI STARTUPS.

Submitted By

Name: MD. ABU AMMAR

Id: 1821944642

Section: 02

Submitted To

Faculty Initial: RkZ

Faculty: Dr. Rokonuzzaman

Department: ECE

Submission Date: December 28, 2020

Data Misguiding AI Startups

Abstract

This article explores the challenges and opportunities presented by advances in artificial intelligence (AI) in the context of AI startups and explores how this advancement of AI, led by the data, creates an illusion for AI entrepreneurs which will misguide their AI startups. The article first examines the ways in which AI evolving. It then dives into some of the limitations of AI's evolving algorithms and threats associated with AI techniques including misguiding deep Neural Networks, and faulty automation. Finally, the paper reviews a number of solutions that could help address the spread of data misguiding AI startups and improve our rational thinking over data thus will reduce the chances for us to fell in the trap of illusion created by the huge collection and resources of data. The article recognizes that to protect AI startups from the data misguiding, there is no single fix.

Keywords

Data– artificial intelligence or AI– IoT – illusion- algorithms – Deep Neural Networks – automated fact– more data or better approach – data without a sound approach become noise.

Introduction

The financial services sector has used customer and contextual data to make better, more informed decisions for many years. With that in mind, it goes without saying that the more data an organization can gather, the better it can protect its interests and create value for itself and its customers. Today, 3.5 billion people own and use a smartphone which collects massive amounts of data from a single endpoint. In fact, the rate at which we as a species create data is exponentially increasing. It's estimated that 90% of all the data in the world was created in the last two years, for example. Internet of Things (IoT) devices may help us process payments, monitor metal fatigue and know when to order printer ink, but all those applications are, at their core, data gathering. IoT devices are sensory endpoints that collect information about the world around them - examples include smart devices, wearables and more. With the number of such devices set to increase dramatically over the coming decade, the amount of data available to everyone from retailers to insurance agencies is set to experience another exponential hike. This vastness of data creates many hypes for the next generation AI technology where innate ability of human being can be transfer into machine to use it in production and process line. Due to the potential money making or profit-making opportunities from such a technology provoke the same exponential growth of AI startups. [1]

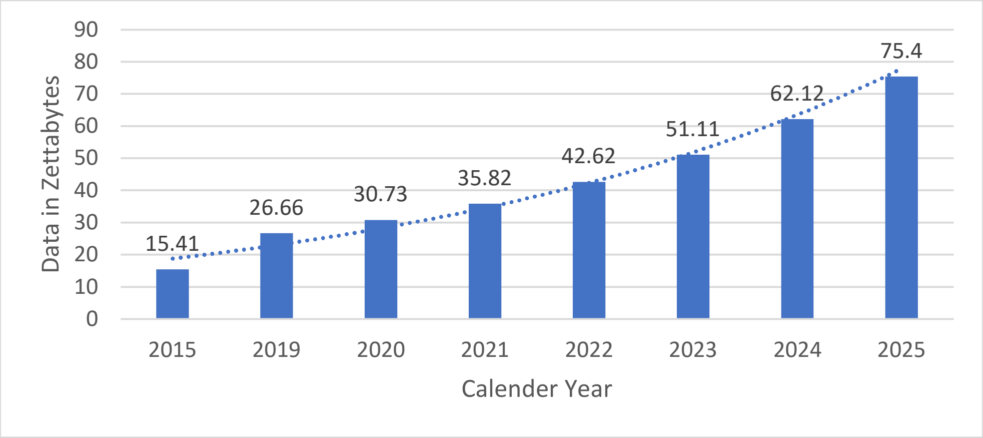
'Garbage In, Garbage Out' (GIGO) a proverb, has been in existence since the invention of computers. But since the invention of artificial intelligence (with its strong needs for data quality), this proverb is more relevant than ever. Artificial Intelligence is highly data-sensitive. For this reason, the quality of data being used on any artificial intelligence process has a significant impact on its success. Let us have a look at how bad data impacts artificial intelligence. Significant advancements in how we collect, archive, and analyze data have progressed AI or Artificial Intelligence. Solving complex problems demands a lot of rich, quality data and fortunately users can now gather it easily, store it cheaply, and process it much faster. From robotic process automation that enhances efficiency to predictive analytics that solve complex problems, technology has fastened the pace for companies looking to be ahead of their competitors. But technology aside, the sophisticated tools that drive these innovations are useless if the data is bad!

Thomas C. Redman denotes that wrong data is the leading enemy to the profitable and widespread use of AI. Training data governs the performance of AI systems. Bad data return bad results. Worse, it flows via AI systems, feeding into the models, and giving out incorrect information.

Now if the data is proven hundred percent accurate then the initial rendering data of AI algorithms of learning is also misguiding as it can match at most 95% an innate ability but failed in the later 5 percent stage which does not bring any success for an AI startup. [2]

High Hopes and Bright Future set the Perfect Stage for Illusion

The evolution of Artificial Intelligence or AI determined by the progress of IoT industry. But what is IoT and why and how it linked with AI, we will unfold the secret now. IoT or the Internet of Things describes the network of physical objects "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet. The definition of IoT has evolved due to the convergence of multiple technologies, real-time analytics, machine learning, commodity sensors, and embedded systems. Traditional fields of embedded systems, wireless sensor networks, control systems, automation (including home and building automation), and others all contribute to enabling the Internet of things. In the consumer market, IoT technology is most synonymous with products pertaining to the concept of the "smart home", including devices and appliances (such as lighting fixtures, thermostats, home security systems and cameras, and other home appliances) that support one or more common ecosystems, and can be controlled via devices associated with that ecosystem, such as smartphones and smart speakers. The internet of things is growing fast and in future people's daily needs going to depend on the internet. It's not just connecting computers and smartphones anymore. Multiple devices that we use in daily life need the internet to serve people. The Internet of Things devices such as machines and sensors are expected to generate 79.4 Zettabytes of data in 2025. Also, IoT will grow at a compound annual growth rate of 28.7% from 2020 to 2025.



According to the projection of the Statista Research Department, 75.44 billion devices will be connected with IoT worldwide by 2025. IoT internet technology is the next major step in making the world a connected place.

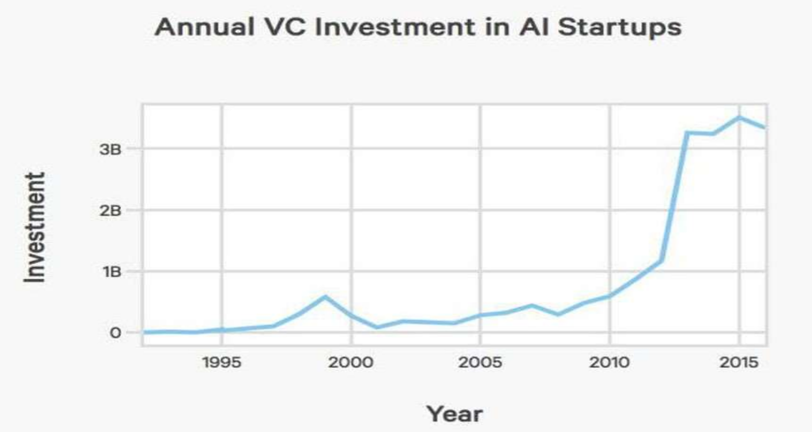
Increased market value: The global IoT market is expected to reach a value of USD 1256.1 billion by 2025 from USD 690 billion in 2019 at a CAGR of 10.53%, during the period 2020-2025. With the development of wireless networking technologies, the emergence of advanced data analytics, a reduction in the cost of connected devices, an increase in cloud platform adoption, the expectation is the market to grow at a positive rate.

5G networks will continue to fuel IoT growth: Major wireless carriers will continue to roll out 5G networks. 5G — fifth-generation cellular wireless — promises greater speed and the ability to connect more smart devices at the same time. Faster networks mean the data accumulated by your smart devices will be gathered, analyzed, and managed to a higher degree. That will fuel innovation at companies that make IoT devices and boost consumer demand for new products. 5G is central to the Internet of Things or a single network for billions of applications. From 2020 to 2030, IoT devices will grow from 75 billion to more than 100 billion, and the improvement from 4G to 5G in terms to grow the Internet of Things is most important. Today's 4G network can support up to 5500 to 6000 NB-IoT devices on a single cell. With a 5G network, up to one million devices can be handled by a single cell.

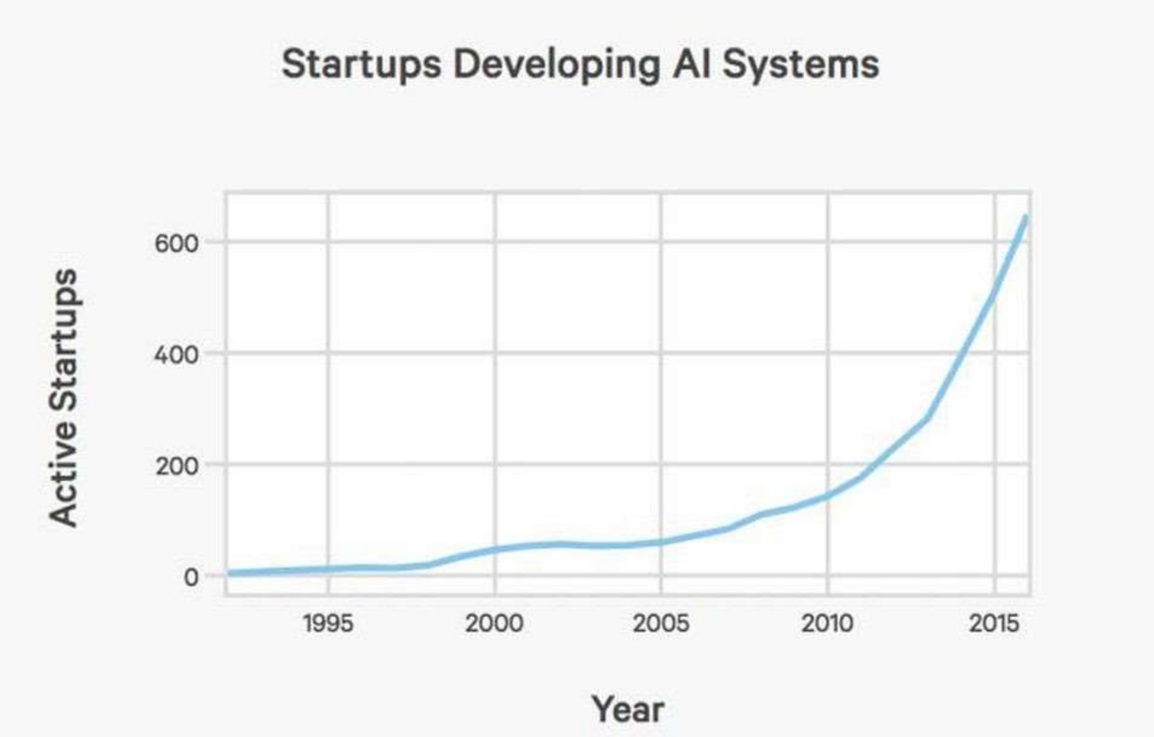
94% of businesses will use IoT by the end of 2021: New reports from Microsoft show almost all businesses will use some form of IoT by the end of next year. The core Internet of Things industries such as manufacturing, retail, transportation, government, and healthcare continue to introduce new Internet of Things applications and solutions to their daily operations.

Growth in the sector of AI: IoT refers to the device that transfers data over a network. This generates unimaginable amounts of data and many organizations are clueless about how to manage this amount of data. To solve this amount of customer data, the Internet of Things allows data flow between the device and AI can help to manage this data without any human errors. Machine Learning is a type of AI (Artificial Intelligence) that helps computers to learn without programming them. The computers are programmed in a way to focuses on data they receive from the device and learn with the received data to understand the customer's preference and adjust itself accordingly.

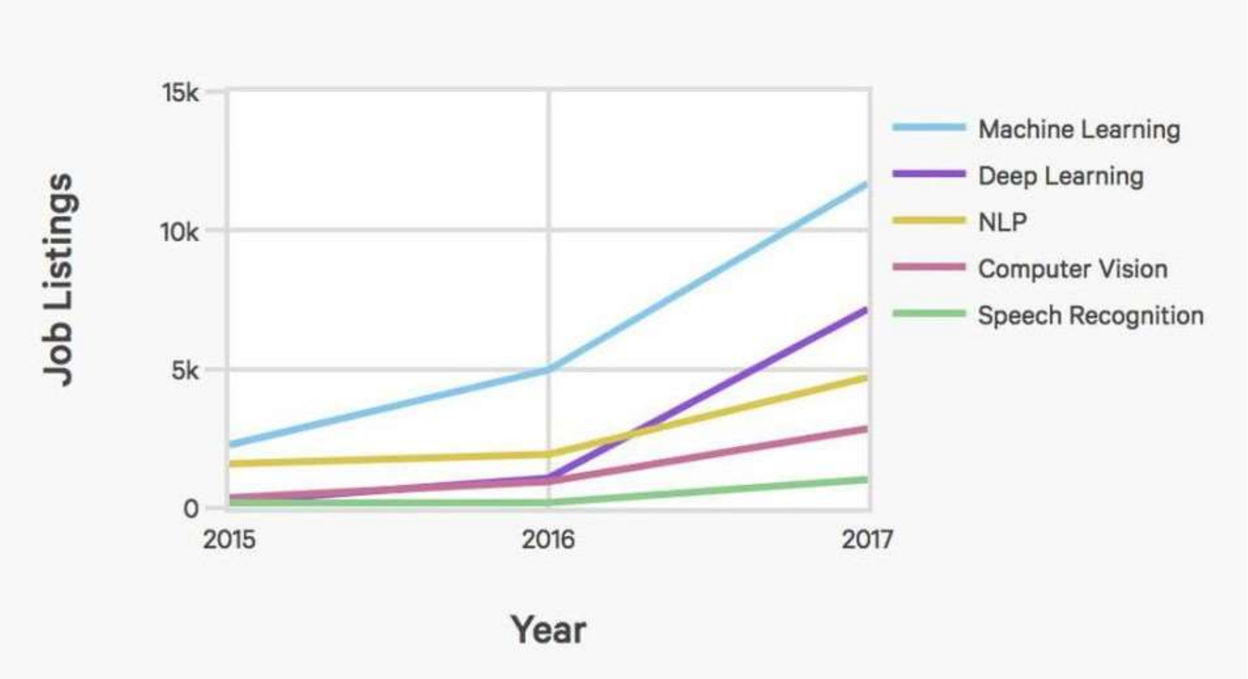
Thus, with the expansion of the Internet of Things, there will also be an expansion in the field of AI. Also, AI is one of the key propellants to the growth of the IoT revolution. Since 2000 there has been 6 times increase in the annual investment level by venture capital or VC investors into US based startups AI startups.



Simultaneously the number of AI startups increased 14 times higher than before. The graph given below illustrate the growing number of AI startups.

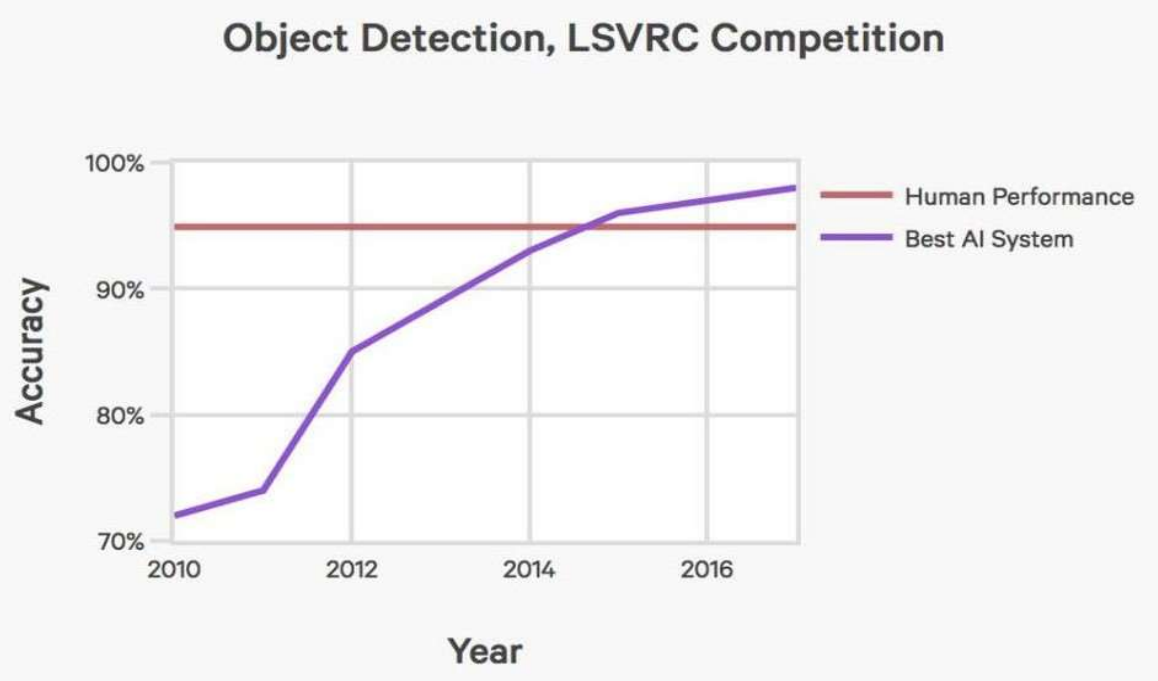


Since AI startups is increasing the job opportunity in different sectors of AI are attracting people all over the world and that increase the job opportunities in AI sectors. Machine Learning, Deep Learning and Natural Language Processing (NLP) are the three most in demand sectors.

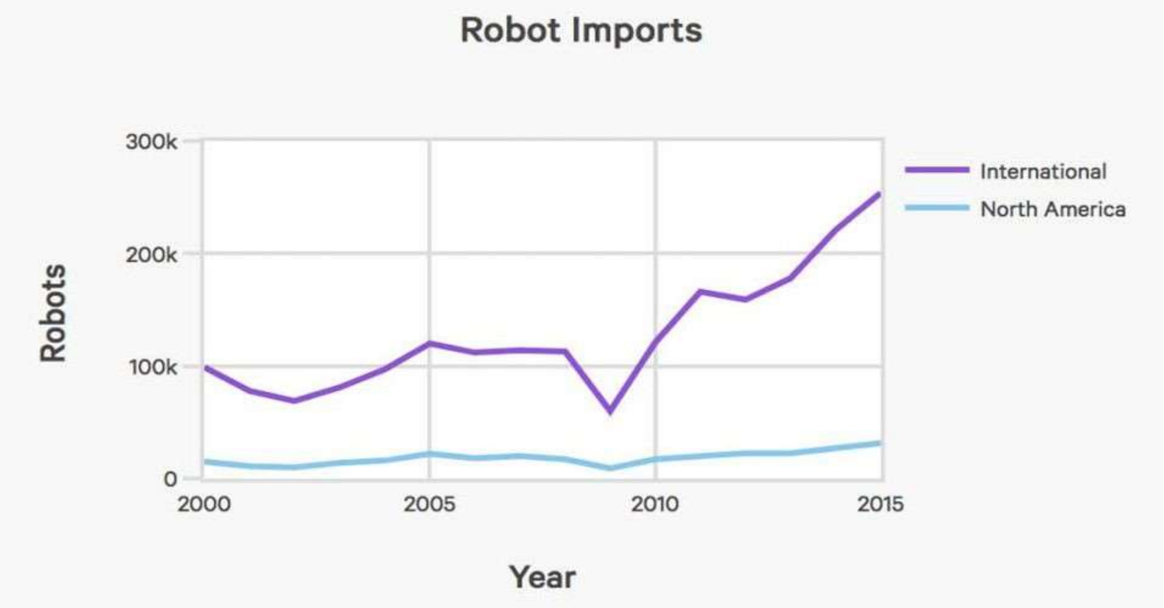


As AI continue to progress the error rates for image labeling has fallen from 28.5 percent to below 2.5 percent from 2010. AI's inflection point for Object Detection task of the Large-Scale Visual

Recognition Challenge (LSVRC) Competition occurred in 2014. On this specific test, AI is now more accurate than human. These findings are from the competition data from the leaderboards for each LSVRC competition hosted on the ImageNet website.



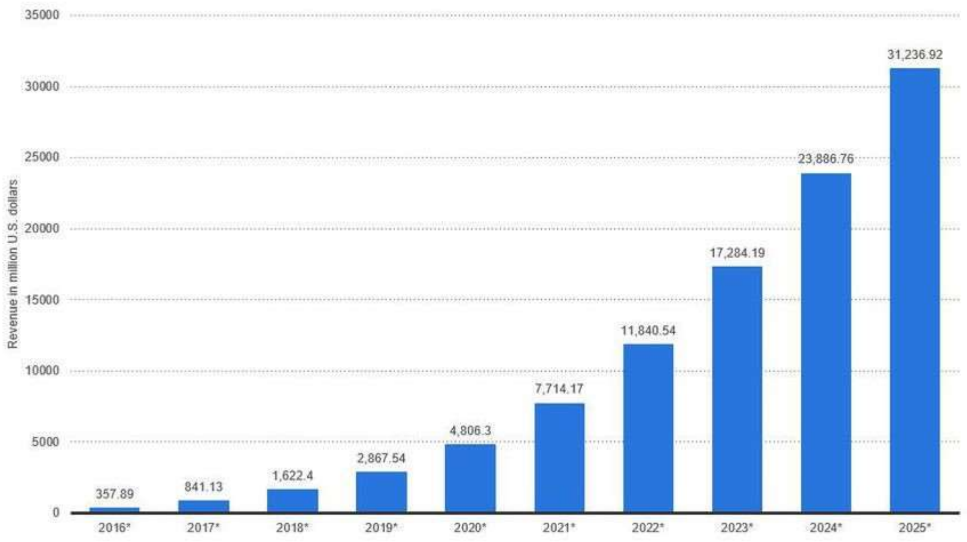
Due to this achievement of AI, robot imports has risen from around 1 lakh to 2.5 lakh from 2000 to 2015 internationally. The data displayed is the number of industrial robots imported each year into North America and Internationally. Industrial robots are defined by the ISO 8373:2012 standard. International Data Corporation (IDC) expects robotics spending to accelerate over the five-year forecast period, reaching \$230.7B in 2021, attaining a Compound Annual Growth Rate (CAGR) of 22.8%.



As a matter of fact, global revenues from AI for enterprise applications is projected to grow from $1.62B in 2018 to $31.2B in 2025 attaining a 52.59% CAGR in the forecast period. Image recognition and tagging, patient data processing, localization and mapping, predictive maintenance, use of algorithms and machine learning to predict and thwart security threats, intelligent recruitment, and HR systems are a few of the many enterprise application use cases predicted to fuel the projected rapid growth of AI in the enterprise.

Enterprise artificial intelligence market revenue worldwide 2016-2025

Revenues from the artificial intelligence for enterprise applications market worldwide, from 2016 to 2025 (in million U.S. dollars)

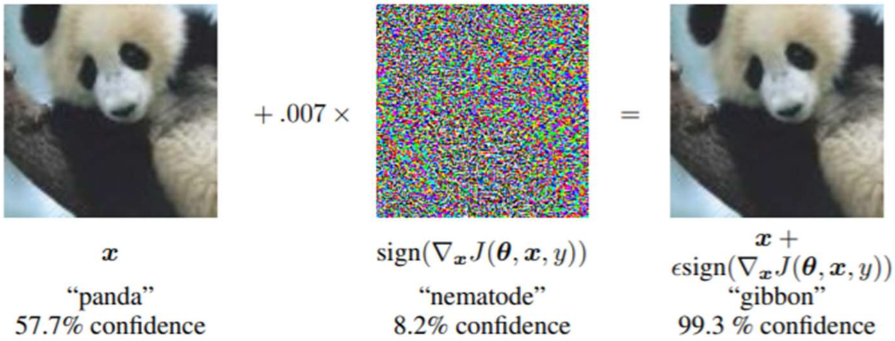


This growth of AI and IoT initially triggers many investors, CEOs, and VCs to invest more on R&D where they would expect engineers can construct the innate ability of human into the machine that can replace human in the production and process which can earn more revenue than with human as IoT devices brings huge amount of data from every end point it seems possible or can say it illustrate the probability in the advanced stage. [3] [4] [5] [6]

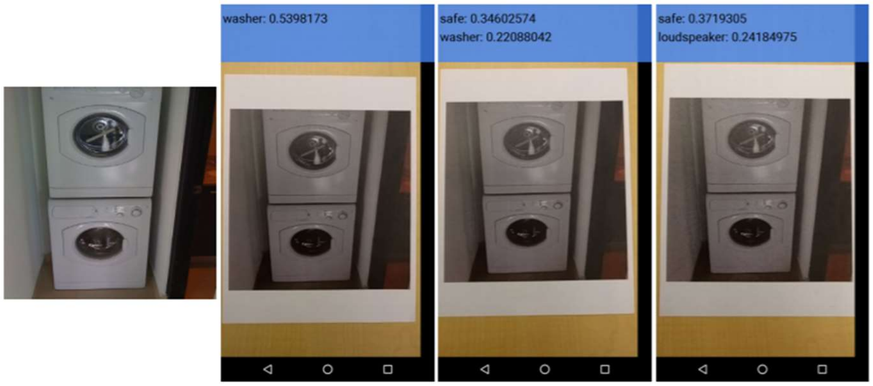
Increasingly Easy Way of Manipulating or Misleading AI Subjects keeps Worsen the Data Misguiding AI Startups

What human can do just in a blink of eyes for machine there needs thousands or millions of instructions to do the same thing. But after those million instructions we may not get the 100 percent accurate output or in between its calculation it may calculate the wrong thing. From the beginning of 21st century, we always try to introduce automation in different things, the most hyped thing was automated car. But is it safe or can it produce benefits in this timeline? To know it’s answer we simply take the current best algorithm to capture a right image. Recent advancements in machine learning and deep neural networks permitted us to resolve complicated realistic problems in images, video, text, genes, or many more. In the current scenario, deep learning-based approaches have overcome traditional image processing techniques. However, misguiding deep neural networks is easy with the help of just one-pixel alteration. That is, artificial perturbations on natural images can easily make DNN misclassify.

Misguiding Deep Neural Networks by Adversarial Examples: In 2015, people at Google and NYU affirmed that ConvNets could easily be fooled if the input is perturbated slightly. For example, our trained model recognizes the "Panda" with a confidence of 58%(approx.) while the same model classifies it as "Gibbon" with a much higher confidence of 99%. This is obviously an illusion for the network, which has been fooled by the noise thus inserted.


$+ .007 \times$
=
$\boldsymbol{x}$
"panda"
57.7% confidence
$\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$
"nematode"
8.2% confidence
$\boldsymbol{x} + \epsilon\text{sign}(\nabla_{\boldsymbol{x}} J(\boldsymbol{\theta}, \boldsymbol{x}, y))$
"gibbon"
99.3 % confidence

In 2017 again, a group of researchers at Google Brain and Ian J. Goodfellow showed that printed images, when captured through the camera and perturbated a slight, resulted in misclassification.



(a) Image from dataset (b) Clean image (c) Adv. image, $\epsilon = 4$ (d) Adv. image, $\epsilon = 8$

The umbrella term for all these scenarios is the Adversarial example.

From the above examples, it is clear that the machine learning models are vulnerable to adversarial manipulations and result in misclassification. In particular, the misguiding of the output of Deep Neural Networks (DNN) can be easily done by adding relatively small perturbations to the input vector. The consideration for pixel attaches as a threat involves:

I. Analysis of the natural images' vicinity, that is, few pixel perturbations can be regarded as cutting the input space using low-dimensional slices.

II. A measure of perceptiveness is a straightforward way of mitigating the problem by limiting the number of modifications to as few as possible.

Mathematically, the problem can be written as-

Let f be the target image classifier which receives n-dimensional inputs,

$x = (x_1, x_2, \ldots, x_n)$, t

$f_t(x)$ is the probability of correct class

The vector $e(x) = (e_1, e_2, \ldots, e_n)$ is an additive adversarial perturbation.

The limitation of maximum modification is L.

$f_{adv}(x + e(x))$ subject to $e(x) <= L$

The Attack: Targeted v/s Untargeted

An untargeted attack causes a model to misclassify an image to another class except for the original one. In contrast, a targeted attack causes a model to classify an image as a given target class. We want to perturb an image to maximize the probability of a class of our choosing.

The Defense

Increasing the Efficiency of the Differential Evolution algorithm such that the perturbation success rates should be improved and comparing the performance of Targeted and Untargeted attacks.

Differential Evolution

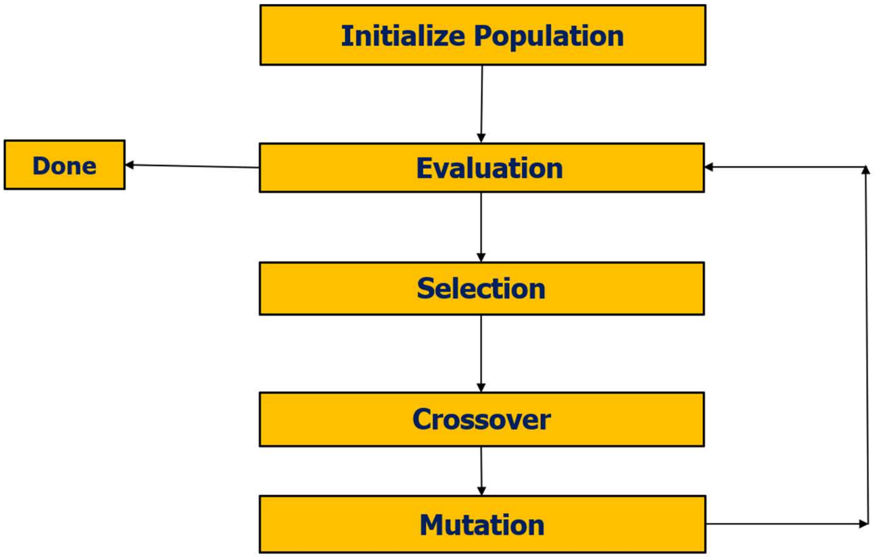
Differential evolution is a population-based optimization algorithm for solving complex multi-modal optimization. Differential Evolution

Moreover, it has mechanisms in the population selection phase that keep the diversity such that in practice, it is expected to efficiently find higher quality solutions than gradient-based solutions or even other kinds of EAs in specific during each iteration another set of candidate solutions (children) is generated according to the current population (fathers).

Why Differential Evolution?

There are three significant reasons to choose for Differential Evolution, viz.,

1. Higher probability of Finding Global Optima,
2. Require Less Information from Target System, and
3. Simplicity



n the context of a one-pixel attack, our input will be a flat vector of pixels, that is,

X= (x_1, y_1, r_1, g_1, b_1, x_2, y_2, r_2, g_2, b_2, …….)

First, we generate a random population of n-perturbations

P= (x_1, x_2…., x_n)

Further, on each iteration, we calculate n new mutant children using the formula

$X_i=x_{r1}+f(x_{r2}-x_{r3})$

such that

$r_1!=r_2!=r_3$

The standard DE algorithm has three primary candidates for improvement: the crossover, the selection, and the mutation operator.

> The selection has been unchanged from the original publication by Storn and Price to state-of-the-art variants of DE, making it less likely that improvements could significantly enhance the performance.

Crossover has a large effect on the search and is of particular importance when optimizing non-separable functions.

Mutation: Can be changed

The mutation operator has been among the most studied parts of the algorithm. Numerous variations published over the years provided all the required background knowledge about the population. It is just a matter of changing some variables or adding some terms to a linear equation. All this makes mutation the best step to improve.

The question then becomes which mutation operator to improve.

The DE/rand/1 operator seems to be the best choice because it is studied extensively, and the comparison of the implementation becomes effortless. Moreover, it would be interesting to see how effectively generating additional training data with dead pixels affects such attacks.

Whatever we put – 1 pixel, some error, noise, fuzz – or anything else, neural networks could give some false recognitions – entirely in an a-priory unpredictable way. [7]

Adversarial examples prove that neural networks are fundamentally broken and can never lead to strong AI. The adversarial images for which only one pixel is altered are challenging to detect by humans. Thus, in this era or timeline we can't expect that an automated car would be available publicly as it has the possibility of unable to detect an instance moment for which a big accident can occur where as a human can easily detect it and can act at that moment to avoid any accident. From the previous section we have seen that IoT has provided us vast level of data but till now we don't have that accuracy in our algorithm so this Data also misguide our AI startups. We can get best lesson from Honda's ASIMO project. At the beginning of 21st century Honda introduced its first humanoid robot ASIMO to aid human to execute their different tasks. Initially it seems a revolutionary achievement as it showed spectacular performance in walking, dancing, and playing. Upon seeing its revolutionary progress Honda invest more and more in their R&D and it was worth $500 million in 18 years long research. Unfortunately, they failed to animate human being's innate ability into machines and this project was dismissed with failure. The reason they had invested that much money in this project was potential revolution it can create and this potential revolution was nothing but an illusion that was created by the Data Misguiding thus it leads to a loss project. [8]

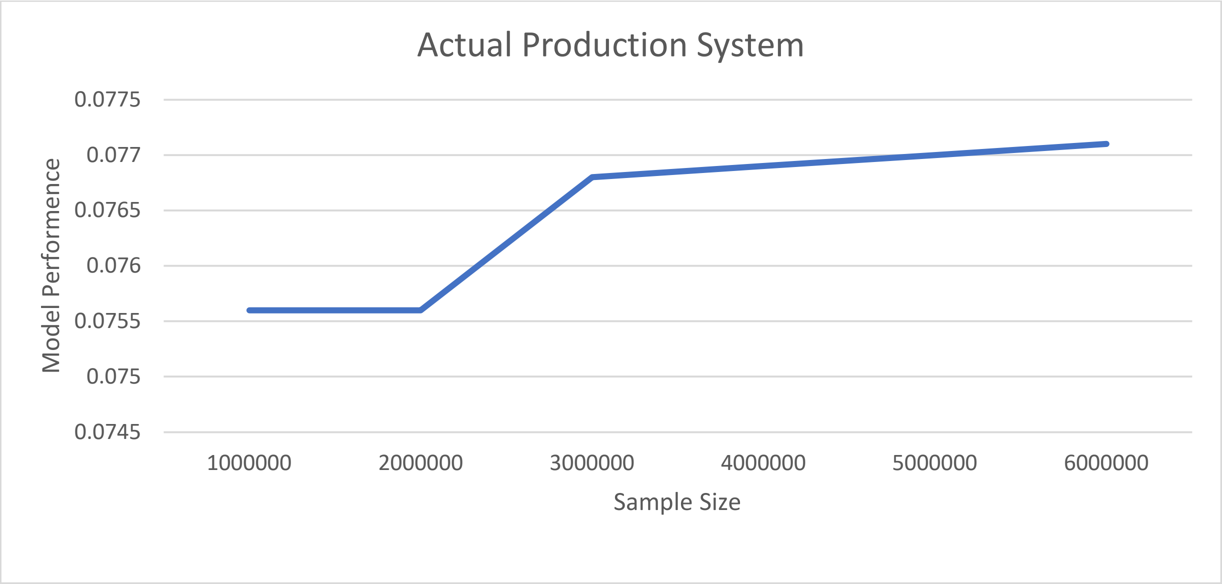
So, What can be Done to Reduce the Misguidance?

When we talk about data misguiding AI startups we need to think over the misguidance of data. How the data can mislead us as when we know numbers don't lie. We got a vast of data from the users but what is better to have in Artificial Intelligence more data or better algorithms. Gross over-generalization of "more data gives better results" is misguiding. Here we explain, in which scenario more data or more features are helpful and which are not. Also, how the choice of the algorithm affects the end result. "In AI, is more data always better than better algorithms?" No. There are times when more data helps, there are times when it doesn't.

Variance or Bias? The basic idea is that there are two possible (and almost opposite) reasons a model might not perform well. In the first case, we might have a model that is too complicated for the amount of data we have. This situation, known as high variance, leads to model overfitting. We know that we are facing a high variance issue when the training error is much lower than the test error. High variance problems can be addressed by reducing the number of features, and yes, by increasing the number of data points. But, in the opposite case, we might have a model that is too simple to explain the data we have. In that case, known as high bias, adding more data will not help.

So, V = (TrE – TE)

And, B = (TE – TrE) where, v= variance; TrE = Training Error; TE = Test Error; B = Bias. See below a plot of a real production system at Netflix and its performance as we add more training examples.



So, no, more data does not always help. As we have just seen there can be many cases in which adding more examples to our training set will not improve the model performance.

More features to the rescue

High bias models will not benefit from more training examples, but they might very well benefit from more features. So, in the end, it is all about adding "more" data, right? Well, again, it depends. Let's take the Netflix Prize, for example. Pretty early on in the game, there was a blog post by serial entrepreneur and Stanford professor Anand Rajaraman commenting on the use of extra features to solve the problem. The post explains how a team of students got an improvement on the prediction accuracy by adding content features from IMDb. In retrospect, it is easy to criticize the post for making a gross over-generalization from a single data point. Even more, the follow-up post references SVD as one of the "complex" algorithms not worth trying because it limits the ability of scaling up to larger number of features. Clearly, Anand's students did not win the Netflix Prize, and they probably now realize that SVD did have a major role in the winning entry. As a matter of fact, many teams showed later that adding content features from IMDB or the like to an optimized algorithm had little to no improvement. Some of the members of the Gravity team, one of the top contenders for the Prize, published a detailed paper in which they showed how those content-based features would add no improvement to the highly optimized collaborative filtering matrix factorization approach. The paper was entitled Recommending New Movies: Even a Few Ratings Are More Valuable Than Metadata. To be fair, the title of the paper is also an over-generalization.

Content-based features (or different features in general) might be able to improve accuracy in many cases. So here we go again, more data does not always help.

Better Data! = More Data

It is important to point out that, better data is always better. The issue is that better data does not mean more data. As a matter of fact, sometimes it might mean less! Think of data cleansing or outlier removal as one trivial illustration of my point. But there are many other examples that are more subtle. For example, we have seen people invest a lot of effort in implementing distributed Matrix Factorization when the truth is that they could have probably gotten by with sampling their data and gotten to very similar results. In fact, doing some form of smart sampling on our population the right way (e.g. using stratified sampling) can get us to better results than if we used the whole unfiltered data set.

Data Without a Sound Approach = Noise

So, am I trying to make the point that the Big Data revolution is only hype? No way. Having more data, both in terms of more examples or more features, is a blessing. The availability of data enables more and better insights and applications. More data indeed enables better approaches. More than that, it requires better approaches. In summary, we should dismiss simplistic voices that proclaim the uselessness of theory or models, or the triumph of data over these. As much as data is needed, so are good models and theory that explains them. But, overall, what we need is good approaches that help us understand how to interpret data, models, and the limitations of both in order to produce the best possible output. In other words, data is important. But, data without a sound approach becomes noise.

Summery and Conclusion

So after this much discussion we can simply analyze that Data can misguide AI startups. And it can only possible when we focus on data more than the approach to utilize it. We always have to remember vastness of data can create only an illusion of a revolution rather than an actual revolution as we have learnt from the past of Honda’s ASIMO and many other tech companies who had invested millions of dollars in research and development in a potential money making or revolutionary project but being ended up as a failed project. This misguidance from data has created a huge loss in many AI startups so far so not fell in this trap of illusion created by the vastness of collection of data we have to analyze the data in an efficient way and always have to keep a fact in mind that more data does not always refers to better data, sometimes small amount of data can be better to perform a task in compare to have more data and in overall we need is good approaches that help us understand how to interpret data, models, and the limitations of both in order to produce the best possible output. In other words, data is important. But, data without a sound approach becomes noise and that can make an illusion of a revolution.

Appendix:

SI	Names of Variables	Definitions	Relationship with other Variables	Real-life Data
1	V	Variance	V depends on the Training and Test Error.	A data model's variance can decide what it needed to execute it more accurately.
2	TrE	Training Error	If Training Error is higher than the Test Error then variance will be higher.	In time of training of an AI object for a data model the total error we find is Training Error.
3	TE	Test Error	If Test Error is higher than the Training Error then variance will be lower.	Before completing an AI object, we test it and in this time the error we get is Test Error.
4	B	Bias	B depends on the Training and Test Error. And B is inversely proportional to V.	If a data model is high bias then it is simpler to explain and it will be accurate if we feed more data.
5	Data	Collection of Data	If variance is higher more data is helpful but if not then the better algorithm will helpful.	For a data model of AI object more collection of data does not improvise that the data is better and data without a sound approach becomes noise.
6	f	Target image classifier	It receives n-dimensional input	It holds all the pixels of an image.
7	$X_1,x_2,\ldots,x_n$	n-dimensional inputs.	These are the inputs of image classifier f.	Every pixels of image is x_i
8	$f_t(x)$	probability of correct class.	Function of x.	It is the probability of an image if its pixel's is correct class.
9	e(x)	additive adversarial perturbation	$e(x) = (e_1, e_2, \ldots, e_n)$.	It is an vector space of an image's additive adversarial perturbation.
10	L	Limitation of maximum modification.	L can be greater than or equal to the vector space e(x).	It is the limitation of maximum modification of an image's pixels.
11	P	Random Population	P is a random population of n-perturbations.	Its calculate random population of n dimensional perturbations of an image's pixels.

References

[1] Egham, "Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020," *Gartner,* August 29, 2019.

[2] SwoopTalent, "How Bad Data Negatively Affects Machine Learning," November 20, 2019.

[3] A. Jyoti, "What is the future of IoT?," November 07, 2020.

[4] I. K. F. U.-N. Eklas Hossain, "Application of Big Data and Machine Learning in Smart Grid, and Associated Security Concerns: A Review," *IEEE,* January 24, 2019.

[5] M. H. u. R. Wazir Zada Khan, "Industrial Internet of Things: Recent Advances, Enabling Technologies, and Open Challenges," *ResearchGate,* November, 2019.

[6] L. Columbus, "10 Charts That Will Change Your Perspective On Artificial Intelligence's Growth," *Forbes,* 2019.

[7] KOPALDEEP, "Misguiding Deep Neural Networks: Generalized Pixel Attack," *Analytics Vidhya,* December 16, 2020.

[8] R. Zaman, "Data Misguiding AI Startups," *The Waves,* August 31, 2020.