

# UNDERSTANDING, DETECTING AND COMBATTING DEEPFAKES IN THE REAL WORLD

**DR YU CHEN**, BASED AT BINGHAMTON UNIVERSITY IN THE US, IS DEVELOPING A MEANS OF UNDERSTANDING AND DETECTING DEEPFAKES IN ONLINE VIDEO SYSTEMS. THE FINDINGS WILL HELP ADVANCE THE RESEARCH FRONTIER OF AUDIO AND VIDEO STREAMING DATA SECURITY

## TALK LIKE AN ELECTRICAL AND COMPUTER ENGINEER

**INTERNET OF THINGS** – a system of interconnected computing devices, mechanical and digital machines, objects, animals or people

**FREQUENCY** – the number of waves, cycles, or vibrations by a body in motion that passes through a fixed point in a given period of time (typically 1 second). For example, 60 cycles in 1 second, resulting in 60 Hz

**POWER DISTRIBUTION NETWORK** – the distribution of electric power from the generating points to the final destination, made of components such as cables and transformers

**NOMINAL FREQUENCY** – the frequency specified for a device (usually 50Hz) for normal operation by the device's manufacturer or supplier

**DEEPFAKE** – superimposing, merging or replacing the likeness of an individual on a subject, and making it appear authentic and real

**EDGE CAMERA RECORDING/STORAGE** – when a device, like a camera, stores recorded information directly on an inbuilt storage system rather than on an external storage device

**BLOCKCHAIN** – a shared, immutable ledger that facilitates the process of recording transactions and tracking assets across computers that are connected as a peer-to-peer network

## PREVALENCE OF DEEPFAKES

The rapid growth of the internet in the 20th century has made it increasingly difficult to know what is true and what is false. Indeed, while conspiracy theories have existed for hundreds of years, online communities enable people to come together to share their theories, with each individual capable of bolstering the strength of the community's belief in what it deems to be true. One notable instance is the increased popularity of the notion that the Earth is flat – this is demonstrably false, but some people are convinced that our planet is a flat rectangle and not a sphere.

Deepfakes and deepfake attacks have only added to the misinformation that is readily available

online. Deepfakes are synthetic media in which existing audio, image or video is replaced with another person's voice or likeness.

Some of these deepfakes are so realistic that it appears as if the person has done or said what the video demonstrates. As the technology used to create deepfakes becomes more sophisticated, the ability to separate fact from fiction becomes increasingly difficult, which can cause significant problems around the world.

It is with this in mind that Dr Yu Chen, based at Binghamton University in the US, is engaged in a project focused on developing a means of understanding and detecting deepfakes in online video systems. The research project aims to help

neutralise the ability of these videos to mislead the public and cause friction between people and even countries.

There is a range of deepfake tools available, thereby enabling people to become anyone, from Elon Musk to Eminem, during video conversations. Almost anyone can use simple video manipulations with modified voices; so, instances of deepfake attacks are on the rise.

"Deepfake video 'attacks', in some public scenarios, have raised more concerns. For instance, in 2017, the start-up Lyrebird posted short audio clips simulating the then US presidential candidates Obama, Trump and Clinton discussing the company's technology with admiration," explains Yu. "Researchers have pointed out that disinformation may cause disturbance in our society and ruin the foundation of trust. More recently, on 17th March 2022, a deepfake video was posted on social media showing Ukraine's President Zelensky calling for his country's soldiers to surrender."

## DETECTING DEEPFAKE ATTACKS

The Electrical Network Frequency (ENF) is an instantaneous frequency in power distribution networks that varies across its nominal frequency of 50/60 Hz, based on power supply and demand from consumers. It has been observed that the surveillance feed contains traces of ENF in both audio and video recordings, so if Yu and his team



## DR YU CHEN

Professor, Department of Electrical and  
Computer Engineering  
Associate Director, Center  
for Information Assurance and  
Cybersecurity, Binghamton University,  
State University of New York, USA

## FIELDS OF RESEARCH

Security, Trust and Privacy in Edge  
Computing and Internet of Things (IoT),  
Smart Cities

## RESEARCH

Developing a means of understanding  
and detecting deepfakes in online video  
systems. The findings will ensure increased  
reliability in what is presented as the truth

## FUNDERS

US National Science Foundation (NSF),  
US Air Force Office of Scientific  
Research (AFSOR),  
Department of Defense

This work is supported by the NSF  
via grant CNS-2039342 and the  
AFOSR Dynamic Data and Information  
Processing Program via grant  
FA9550-21-1-0229. The views  
and conclusions contained herein are  
those of the authors and should not be  
interpreted as necessarily representing  
the official policies or endorsements,  
either expressed or implied, of the US  
Air Force.

approaches to theoretically prove the effectiveness  
and robustness of their approach. Ultimately, Yu's  
research will help to combat the rise of 'fake news'  
in an era where people doubt the veracity of that  
which is true and believe false information.

can detect these traces, they can determine  
whether the video and audio are real or fake.

"In this research, ENF signals are extracted  
from video/audio recordings generated by edge  
cameras connected to the power grid. The  
authenticity of ENF signals is validated using  
signal traces collected at multiple locations within  
the same power grid," says Yu. "Next, a dynamic  
cross-correlation coefficient is adopted that  
verifies the authenticity of the ENF estimate  
with a parallel ground truth ENF estimate from  
the main power grid."

The team has worked on building and testing a  
proof-of-concept prototype using real-world  
scenarios and the experimental results have  
been analysed to verify the effectiveness and  
correctness of the proposed detection scheme.

## WHAT MAKES YU'S METHOD OF DEEFAKE DETECTION NOVEL?

It is a continuous battle between the  
development of deepfake technology and the  
development of deepfake detection methods.  
The countermeasures and mitigation tools  
available for detection are still in their infancy.  
Often, it is enough to catch inconsistencies in  
audio and video streaming (AVS), such as subtle  
facial expressions that are not realistic, using  
machine learning.

Artificial intelligence (AI) can be employed to  
make fake audio and video sound and look even  
more real. "Instead of engaging in the endless  
AI 'arms race' where we fight fire with fire, our  
research approaches the problem from a different  
standpoint," explains Yu. "Our method delivers a  
disruptive technology that enables the ultimate  
victory in the battle against deepfake attacks."

Apart from the obvious benefits of being able  
to distinguish between what is real and what  
is fake, the success of the research will also  
advance the research frontier of AVS data  
security. "The results from our studies will  
enable more novel Internet of Video Things  
(IoVT) and edge computing-based applications  
to be developed," says Yu. "This is essential for  
mission-critical delay-sensitive applications,  
where fake video inputs will cause disastrous  
consequences, including kinetic military  
action, law enforcement, civil protection,  
disaster relief, social movements, business  
teleconferences and many others."

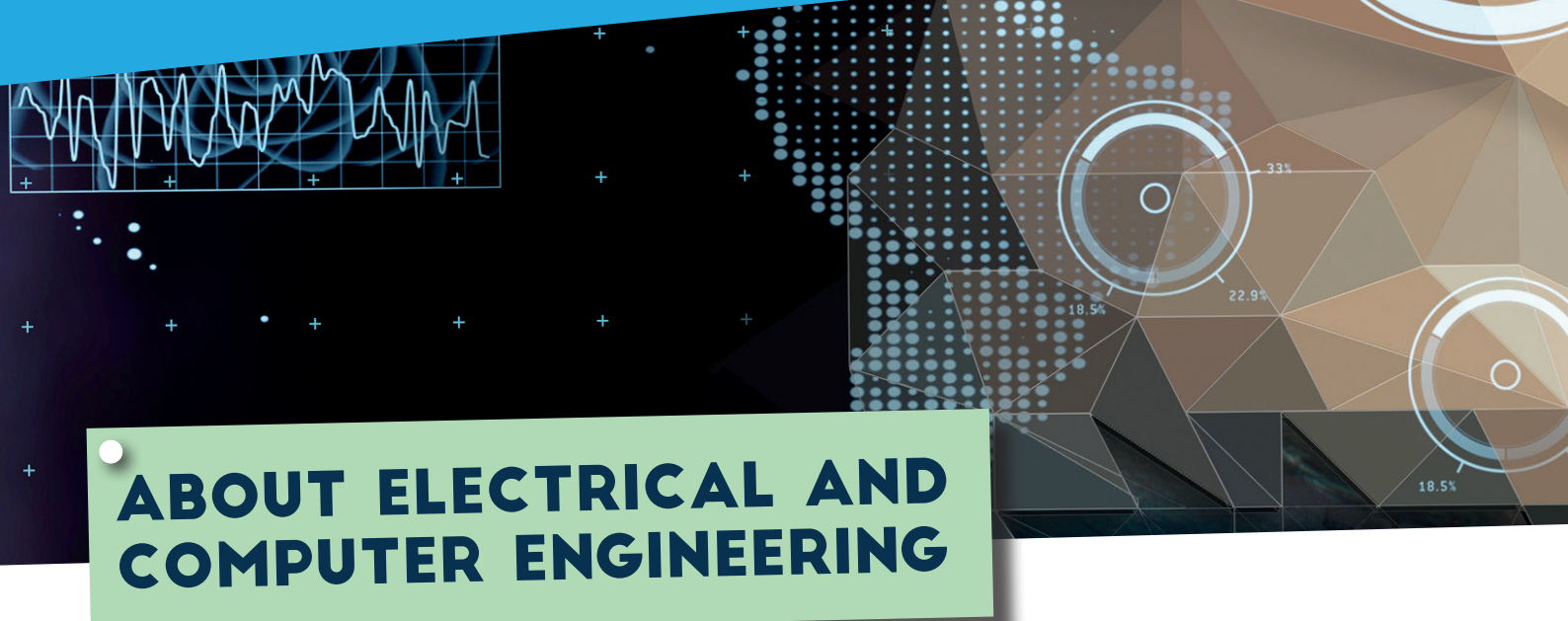
So far, the team has validated the correctness  
and effectiveness of the ENF-based detection  
algorithms for two scenarios. One is a proof-  
of-concept prototype tested with deepfaked  
audio and video authentication in an online video  
conferencing setup and verifies the feasibility of  
the system called DeFakePro.

The other is a Lightweight Environmental  
Fingerprint Consensus (LEFC)-based  
detection of compromised smart cameras in  
edge surveillance systems. By integrating a  
novel blockchain-based consensus protocol,  
the DeFakePro and LEFC schemes can detect  
deepfaked video/audio inputs in real-time.

## WHAT ARE THE NEXT STEPS FOR THE RESEARCH?

The team is engaged in multiple ongoing tasks,  
including the detection of deepfaked video, audio  
and photos on social media or other sites. In  
addition, they are working on developing a deeper  
understanding of the robustness of the proposed  
methods for use in forensics. Yu and his team  
also want to develop information theory-based





# ABOUT ELECTRICAL AND COMPUTER ENGINEERING

As Yu's research shows, the field of electrical and computer engineering can lead to the development of technologies that make the world a better place. Computers and computing technologies are developing at such a rate that there will always be new challenges arising from one day to the next, so scientists and engineers working within the field will always have something to do. You can take your career in so many different directions, which means that it is up to you what pathway you choose to take after you have obtained your degree – or you can instead decide to take a work placement that will give you real-world experience.

## WHAT DOES YU FIND REWARDING ABOUT RESEARCH IN HIS FIELD?

Yu reveals that it is hugely satisfying to find, design and invent new solutions to tackle cutting-

edge challenges. "I love working to help humans and society move forward," he explains. "I find that helping society enter into a safer, more secure and more convenient mode of living in the future is what inspires me daily."

## WHAT CAN THE NEXT GENERATION OF ELECTRICAL AND COMPUTER ENGINEERS EXPECT TO BE WORKING ON IN THE FUTURE?

As intelligent information and communication technologies are continuously and pervasively woven into the daily operations of the world, the next generation of electrical and computer engineers will become increasingly indispensable. "I envisage the next generation of electrical and computer engineers will design, implement, manufacture, test, maintain and secure the critical infrastructures which form the solid

**"I LOVE WORKING TO HELP HUMANS AND SOCIETY MOVE FORWARD."**

foundation of modern human society," says Yu.

If you want to become part of an increasingly exciting field that will only become more important in the future then electrical and computer engineering might just be the research field for you!



## EXPLORE CAREERS IN ELECTRICAL AND COMPUTER ENGINEERING

- The Institution of Engineering and Technology has a student hub which contains loads of useful information: [www.theiet.org/career/routes-to-engineering/student-hub/](http://www.theiet.org/career/routes-to-engineering/student-hub/)
- Electrical Careers is a resource focused on the industry which will show you the options available to you: [www.electricalcareers.co.uk](http://www.electricalcareers.co.uk)
- According to Payscale, the average salary in the US for Electrical Engineers is \$79,163 and \$87,753 for Computer Engineers.

## PATHWAY FROM SCHOOL TO ELECTRICAL AND COMPUTER ENGINEERING

- Yu suggests that students wishing to pursue a career in the field should focus on taking mathematics, physics and programming – if your school offers it.
- Two or three A levels, or equivalent, for a degree.
- You could do a Level 4 and 5 Higher National Diploma in Electrical and Electronic Engineering at college before looking for work. To take this route, you'll need one or two A levels, a Level 3 diploma or relevant experience. You can find more information on Prospects: [www.prospects.ac.uk/careers-advice/what-can-i-do-with-my-degree/electrical-and-electronic-engineering](http://www.prospects.ac.uk/careers-advice/what-can-i-do-with-my-degree/electrical-and-electronic-engineering) or on the UK national careers website here: [nationalcareers.service.gov.uk/job-profiles/electrical-engineer](http://nationalcareers.service.gov.uk/job-profiles/electrical-engineer)

# MEET DEERAJ



**DEERAJ NAGOTHU**

**PhD Student**

*Electrical and Computer Engineering*

**As a group, we focus on enhancing the IoT/edge computing devices with modern technologies like blockchain and artificial intelligence (AI).**

My role as a researcher is focused on secure authentication of media transmissions and preserving information integrity against audio and visual layer attacks in edge devices. Frame forgeries enhanced by AI can significantly alter the perception of events by creating false realities and threatening our information security and privacy. My work aims to create a solution to distinguish the fake from the original using a unique environmental fingerprint technique.

**A typical day consists of reading new publications to widen the scope of our research,** designing and conducting experiments with new algorithms, and measuring how it fares against the media forgeries, which typically involves coding in multiple languages for the development and deployment stages.

**While pursuing my master's degree, I started my academic research on Network Computer Security.** My research aimed to study the network attacks that are launched through web browsing, so I created a Honey-pot (Decoy) system to browse unsecured networks and discover zero-day exploits. I had also developed an interest in modern computer vision applications using Deep Learning. I realised how easy it could be to create a media forgery attack and deploy it in networked devices like surveillance systems that solely depend on their visual input for security. This led to developing my thesis on securing the multimedia in edge devices using techniques that are extremely hard for a Deep Learning model to replicate and forge.

**I have interests in landscape and astrophotography, which is where my interests in images developed.** I have also been involved in many robotics projects during my bachelor's

degree. Recently, I have spent some personal time developing a mini self-driving car using computer vision.

**Dr A.P.J Abdul Kalam, an aerospace scientist and the 11th President of India,** and my father are my inspirations, who taught me to value education and hard work in becoming an excellent scientist.

**I love to explore new knowledge fields, constantly learning and teaching** (which helps figure out the holes in my knowledge), working without getting distracted and, most importantly, being persistent.

**I want to research cutting-edge technology in AI development** and its secure integration into our environment, moving forward, leading to becoming a well-published writer in academic literature.

## HOW DID YOU BECOME AN ELECTRICAL AND COMPUTER ENGINEER?

**WHAT WERE YOUR INTERESTS WHEN YOU WERE GROWING UP?**

I love history – reading allows me to live different lives and recognise what the most important things in my life are. I was also curious to figure out what happens inside machines. I disassembled my grandpa's TV when I was a kid, but when I tried to put it back together, I found there were a few small pieces leftover!

**WHO OR WHAT INSPIRED YOU TO BECOME AN ENGINEER?**

When I was a third-grade pupil in elementary school, a book that described how the Wright brothers invented, built and flew the world's first airplane opened my eyes to the amazing things that engineers can do.

**WHAT ATTRIBUTES HAVE MADE YOU SUCCESSFUL AS AN ENGINEER?**

I guess the most critical factors are maintaining curiosity and the capacity to pick up new knowledge and skills when needed.

**HOW DO YOU TAKE A BREAK FROM YOUR WORK?**

My main activity is reading history books, specifically the history of technology. I am particularly interested in the development of humans over time, and how we have evolved to make and do truly amazing things. Gardening also brings me a lot of pleasure – being close to nature has a calming effect and helps me to cope with the stress of working life!

**WHAT ARE YOUR PROUDEST CAREER ACHIEVEMENTS SO FAR?**

I am a firm believer that the proudest achievement is always the next milestone – this mindset keeps me on my toes and encourages me to keep moving forward with my research.

### YU'S TOP TIPS

1. It is important to build a solid foundation of the fundamentals before pursuing more nuanced areas of enquiry.
2. Keep an open mind and do not be easily offended by differences of opinion – always be open to saying yes.
3. Do not work so hard that you burn yourself out; it is OK to play games or enjoy books outside of your research!