Enhancing Synthetic Media Detection and Mitigation for Thwarting Election Interference with the United States Cyber Command

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

Jacob Locklear is a Business Systems Analyst for CACI International Inc. He is an undergraduate student pursuing a Bachelor of Science degree in Management Information Systems and a former student participant in the PREP Program at George Mason University's Costello College of Business (Fairfax County, Virginia, USA).

Ritika Dixit is a Business Analyst for the Commonwealth of Kentucky. She is an undergraduate student pursuing a Bachelor of Business degree in Management Information Systems at George Mason University's Costello College of Business (Fairfax County, Virginia, USA).

----- ***Industry Participant / Mentor*** -----

Alison Ward
Analyst
United States Cyber Command

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
Instructional Faculty & Dean's Teaching Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

---- Client Testimonial ----

“The students delivered an impactful, and innovative solution, which aligned directly with U.S. Cyber Command's mission to secure our nation's cyber domain. Their contributions highlighted critical information on current, and future challenges in cyberspace. The student's dedication, professionalism, and client-centric approach showcased the role academic research provides to stay ahead of emerging threats, and maintain resilient cyber defenses.”

- Alison Ward | United States Cyber Command

Introduction

The U.S. Cyber Command, a combatant of the U.S. Department of Defense, tasked us with examining how key foreign adversaries use emerging technologies to influence U.S. elections. This project focused on exploring the use of synthetic media and deepfakes to influence U.S. elections. With foreign adversarial groups using Artificial Intelligence (AI) technologies to spread false information as a main focus, the team worked on identifying ways to detect and mitigate these threats, improving election integrity and security. This directly aligns with the Cyber Command's mission which focuses on securing cyberspace.

Business Challenge

Deepfakes are fake videos, images, or audio made using artificial intelligence that look and sound real. These are increasingly used by foreign groups to spread false information about candidates or elections, confusing voters and interrupting the democratic process. The main challenge is that AI is advancing rapidly, and models are being trained to use internet data to produce higher quality content. Therefore, deepfakes are getting better and harder to detect and respond to.

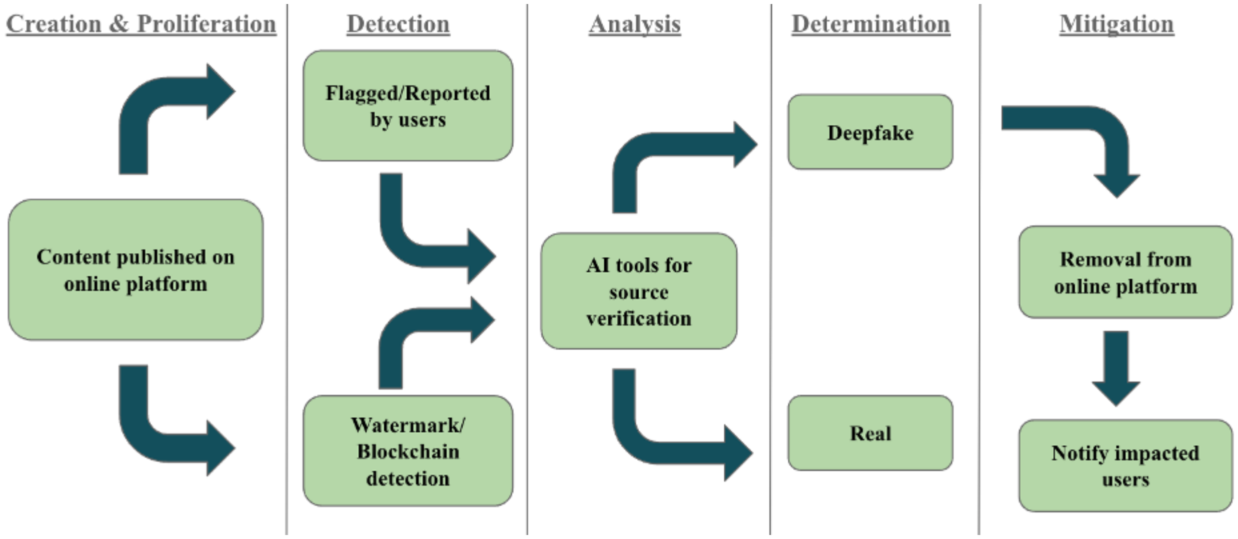
Activities Done to Address the Business Challenge

During our 10 weeks of work with US Cyber Command, we performed the following activities:

- Researched how deepfake and synthetic media have been used in past elections.
- Analyzed recent incidents, like a fake video of Nancy Pelosi and a fake phone call using Joe Biden's voice, to understand their impact.
- Studied tools and strategies, such as blockchain and watermarking, that can help detect fake content.
- Performed research on regulatory policies involving deepfake political content to understand current federal and state laws.
- Developed the ***Deepfake Analysis and Detection (DAD) Framework***, a five-phase approach to help online platforms detect deepfake content and mitigate the impact on public perception.
- Applied the DAD framework to a recent deepfake political incident to demonstrate its use.

Results & The Positive Impact

The Deepfake Analysis & Detection (DAD) framework is applicable to any online platform that allows users to publish content. The goal of the DAD framework is to allow for effective identification of synthetic media using AI tools and mitigate the impact on public perception.


Creation & Proliferation
Detection
Analysis
Determination
Mitigation
Content published on online platform
Flagged/Reported by users
Watermark/ Blockchain detection
AI tools for source verification
Deepfake
Real
Removal from online platform
Notify impacted users

In the **Creation and Proliferation** phase, content is published on an online platform and is being spread rapidly, impacting public perception on a large scale. In the **Detection** phase, suspicious content is flagged either by platform users or the detection of watermarking and blockchain technology (implemented by the online platform) for further inspection. In the **Analysis** phase, platforms leverage AI tools to investigate the source of content and assess credibility. In the **Determination** phase, a decision is made on content authenticity. And in the **Mitigation** phase, the platform can potentially remove the inauthentic content. In addition, any user who viewed the content is promptly notified through the online platform to mitigate the impact on public perception.

The team's research led to practical solutions, including:

- A clear framework (the DAD Framework) for detecting and reducing the impact of deepfake content.
- New ideas for how companies and lawmakers can work together to prevent fake content from spreading.
- Raising awareness for the negative impact deepfakes can have and the importance of an agile response to stop these threats.
- The potential to share our findings and proposed solutions in **the ISACA Journal**, helping professionals understand and address these critical issues globally.

Conclusion

Synthetic media has been an acute and escalating threat to the integrity of the election process in U.S. elections over the years. Foreign entities are systematically using artificial intelligence to interfere in elections, requiring coordinated national efforts to combat these activities. The proposed DAD framework facilitates a straightforward approach to deepfake detection and mitigation, specifically for online platforms. Through the DAD framework, a prompt and clear response limits the false public perception that deepfakes can create. With the unified efforts between the private and public sectors, stronger safeguards can be built that protect elections in an increasingly digital world. Publishing this research in the **ISACA Journal** would further expand its impact, providing actionable insights for cybersecurity and technology professionals worldwide.

PREP Student Reflection

This project was a great learning experience. It helped us understand the real-world impact of AI technology and gave us the chance to work on solutions for a real critical issue prompted by an organization. We gained real world experience communicating and collaborating with a Department of Defense client and learned a lot about teamwork, problem solving, and how to apply what we have studied in class to an important topic. The takeaways from this experience will be beneficial to our professional careers post-graduation from George Mason University. Working with the U.S Cyber Command made us realize how important it is to use technology responsibly to protect the democratic process of U.S elections. The possibility of publishing our findings in ISACA has been an exciting and motivating part of this project, showing how academic work can make a broader difference in the practitioner's world.