NEWS RELEASE 29-APR-2021

Breakthrough Army technology is a game changer for deepfake detection

U.S. ARMY RESEARCH LABORATORY

Science Business Announcement

ADELPHI, Md. -- Army researchers developed a Deepfake detection method that will allow for the creation of state-of-the-art Soldier technology to support mission-essential tasks such as adversarial threat detection and recognition.

This work specifically focuses on a lightweight, low training complexity and high-performance face biometrics technique that meets the size, weight and power requirements of devices Soldiers will need in combat.

Researchers at the U.S. Army Combat Capabilities Development Command, known as DEVCOM, Army Research Laboratory, in collaboration with Professor C.-C. Jay Kuo's research group at the University of Southern California, set out to tackle the significant threat that Deepfake poses to our society and national security. The result is an innovative technological solution called DefakeHop. The researchers worked under the laboratory director's Research Award for External Collaborative Initiative and the Army AI Innovation Institute.

Their work is featured in the paper titled "DefakeHop: A light-weight high-performance deepfake detector," which will be presented at the IEEE International Conference on Multimedia and Expo 2021 in July.

Deepfake refers to artificial intelligence-synthesized, hyper-realistic video content that falsely depicts individuals saying or doing something, said ARL researchers Dr. Suya You and Dr. Shuowen (Sean) Hu. Most state-of-the-art deepfake video detection and media forensics methods are based upon deep learning, which have many inherent weaknesses in terms of robustness, scalability and portability.

"Due to the progression of generative neural networks, AI-driven deepfake advances so rapidly that there is a scarcity of reliable techniques to detect and defend against deepfakes," You said. "There is an urgent need for an alternative paradigm that can understand the mechanism behind the startling performance of deepfakes and develop effective defense solutions with solid theoretical support."

Combining team member experience with machine learning, signal analysis and computer vision, the researchers developed an innovative theory and mathematical framework, the Successive Subspace Learning, or SSL, as an innovative neural network architecture. SSL is the key innovation of DefakeHop, researchers said.

"SSL is an entirely new mathematical framework for neural network architecture developed from signal transform theory," Kuo said. "It is radically different from the traditional approach, offering a new signal representation and process that involves multiple transform matrices in cascade. It is very suitable for high-dimensional data that have short-, mid- and long-range covariance structures. SSL exploits such a property naturally in its design. It is a complete data-driven unsupervised framework, offers a brand new tool for image processing and understanding tasks such as face biometrics."

Most current state-of-the-art techniques for deepfake video detection and media forensics methods are based on the deep learning mechanism, You said.

According to the team, DefakeHop has several significant advantages over current start-of-the-arts, including:

-It is built upon the entirely new SSL signal representation and transform theory. It is mathematically transparent since its internal modules and processing are explainable

-It is a weakly-supervised approach, providing a one-pass (without needing backpropagation) learning mechanism for the labeling cost saving with significantly lower training complexity

-It generates significantly smaller model sizes and parameters. Its complexity is much lower than that of state-of-the-art and it can be effectively implemented on the tactical edge devices and platforms

-It is robust to adversarial attacks. The deep learning based approach is vulnerable to adversarial attacks. This research provides a robust spatial-spectral representation to purify the adversarial inputs, thus adversarial perturbations can be effectively and efficiently defended against

This research supports the Army's and lab's AI and ML research efforts by introducing and studying an innovative machine learning theory and its computational algorithms applied to intelligent perception, representation and processing, You said.

"We expect future Soldiers to carry intelligent yet extremely low size-weight-power vision-based devices on the battlefield," You said. "Today's machine learning solution is too sensitive to a specific data environment. When data are acquired in a different setting, the network needs to be re-trained, which is difficult to conduct in an embedded system. The developed solution has quite a few desired characteristics, including a small model size, requiring limited training data, with low training complexity and capable of processing low-resolution input images. This can lead to game-changing solutions with far reaching applications to the future Army."

The researchers successfully applied the SSL principle to resolve several face biometrics and general scene understanding problems. Coupled with the DefakeHop work, they developed a novel approach called FaceHop based on the SSL principle to a challenging problem-recognition and classification of face gender under low image quality and low-resolution environments.

The team continues to develop novel solutions and scientific breakthroughs for face biometrics and for general scene understanding, for example, target detection, recognition and semantic scene understanding.

"We all have seen AI's substantial impact on society-both good and bad, and AI is transforming many things," Hu said. "Deepfake is an adverse example. The creation of sophisticated computer-generated imagery has been demonstrated for decades through the use of various visual effects in the entertainment industry, but recent advances in AI and machine learning have led to a dramatic increase in the realism of fake content and the ease of access to these tools."

The research team has the opportunity to address these challenging issues, which have both military and every day impact.

"We see this research as new, novel, timely and technically feasible today," You said. "It is a high risk, high innovation effort with transformative potential. We anticipate that this research will provide solutions with significant advantages over current techniques, and add important new knowledge to the sciences of artificial intelligence, computer vision, intelligent scene understanding and face biometrics."

###

Related papers:

FaceHop: A light-weight low-resolution face gender classification method, ICPR Workshop on Mobile and Wearable Biometrics (WMWB 2020), January 10-15, 2021

Pixelhop++: A Small Successive-Subspace-Learning-Based (SSL-Based) Model For Image Classification, IEEE International Conference on Image Processing (ICIP), December 2-28, 2020

Media Contact

Jenna Brady
jenna.c.brady.civ@mail.mil
301-394-1819

@ArmyResearchLab

http://www.arl.army.mil