Sensitive Material Privacy Safeguard for Unmanned Aerial Vehicles

Mel Jesson Cabrera, Bethune-Cookman University, FL
Co-Author: Dalton Mitchum, Embry-Riddle Aeronautical University, FL

An article published by Wired Magazine in 2012 states that the military discovered that unknown militants were tapping into the drone feeds. This problem gained attention back in 2008, when it was discovered that militants in the Middle East were able to gain military drone feed using equipment as cheap as $25. In the year 2014, the company Amazon proposed the idea of utilizing drones to deliver packages to Federal Administration (FAA), with Walmart proposing a similar request in 2015. These two cases are only the tip of the iceberg when comes to the amount of permit requests from companies the FAA has received. With each year, Unmanned Aerial Vehicles (UAVs) have become more widely used among both businesses, consumers, and governments. However, the widely utilization of UAVs also raises privacy concerns, because most UAVs' have high resolution cameras, which can capture videos with sensitive information from individuals, such as faces, debit/credit cards, license plates, etc. caught on video. Therefore, it is highly desirable to remove the sensitive information from video/pictures captured by UAVs.

Methods: To protect the right of privacy for individuals, this research proposes a Field Programmable Gate Array (FPGA) based system that can detect and block sensitive objects from UAVs' video data. Our system can be integrated into UAVs to directly remove the sensitive information from their captured video data. Specifically, the FPGA will run the algorithm based on the Viola-Jones object detection and process images at certain frames in the video feed and block sensitive material. The proposed system will then create a duplicate video with the sensitive objects blocked and then delete the original video captured by the feed. As a result, only non-sensitive information will be presented in the final video data.

Results: We implemented our proposed system using MATLAB. Our results demonstrate that our system can block objects and people effectively and efficiently. Meanwhile, the processing cost of our system increases with the size of video footage. This finding motivates our future research to enhance the scalability of our system.

Conclusion and Future Research: The fourth amendment, the right to privacy is one of the most important individual rights that we have in our society and spawning a sector in the economy based on preserving it. With the rising mainstream popularity of UAS, common use of drones adds a new dimension to privacy protection due to the surveillance capabilities of commercial UAS whether intended use or not. With the visual privacy guard system (VPG) proposed in this research, we provide a solution to the privacy problem spawned by the mainstream use of UAVs in our daily lives. Further research involves effective methods in reducing processing power consumption and overall power consumption, factors that may help increase efficiency in the proposed system.

References:
Viola, Paul, Michael Jones, 2001, Rapid Object Detection Using a Boosted Cascade of Simple Features, Proc. IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Kauai, HI, Vol. 1, pp. I-511 - I-518.
J. A. Steinmann, R. F. Babiceanu and R. Seker, "UAS security: Encryption key negotiation for partitioned data," 2016 Integrated Communications Navigation and Surveillance (ICNS), Herndon, VA, 2016, pp. 1E4-1-1E4-7.
M. A. Alghumgham, R. F. Babiceanu and R. Seker, "Ascertain privacy conservation and data security protection onboard small UAS," 2016 Integrated Communications Navigation and Surveillance (ICNS), Herndon, VA, 2016, pp. 1E3-1-1E3-8.
R. F. Babiceanu, P. Bojda, R. Seker and M. A. Alghumgham, "An onboard UAS visual privacy guard system," 2015 Integrated Communication, Navigation and Surveillance Conference (ICNS), Herdon, VA, 2015, pp. J1-1-J1-8.

Funder Acknowledgement(s): This research is supported by the NSF REU grant (# 1757781). I also thank Dr. Jiawei Yuan and Dr. Radu Babiceanu at ERAU for their advising and help.

Faculty Advisor/Mentors: Radu F. Babiceanu, Radu.Babiceanu@erau.edu. Jiawei Yuan, yuanj@erau.edu