IMAGE VERIFICATION AND SURVEILLANCE ANALYSIS USING MACHINE LEARNING

STEVEN KADNER, R. MICHAEL WHITE, MARKKU KOSKELO, JUDY BECKES TALCOTT, STEPHEN CRIM, AND NOAH KADNER
INTRODUCTION

• Present IAEA process.
  – Use of General Advanced Review Station (GARS) software to identify scene change anomalies and areas of interest within archival surveillance video images.
  – Areas of the video scene changes are deterministic, e.g., fixed areas and pre-determined changes that are to be flagged.
  – No method to analyze video stream real time, even if the images are being transmitted to the IAEA HQ.
  – No method to detect anomalies that are outside the pre-determined scenarios.
TECHNOLOGY DEVELOPMENT SINCE GARS

• High-performance image analysis and computer vision techniques with Artificial Intelligence (AI) or now more popularly named Machine Learning (Core ML) with support for
  – over 30 layer types
  – standard models such as tree ensembles, Support Vector Machines, and generalized linear models
  – face tracking, face detection, detection of people in general, detection of landmarks and landscape features, text detection, rectangle detection, barcode detection, object tracking (vehicles), and image registration
  – easy integration with existing open source machine learning models including: Places205-GoogLeNet, ResNet50, Inception v3, and VGG16
  – machine learning to deeply understand text using features such as language identification, tokenization, lemmatization, part of speech, and named entity recognition
APPLICATION TO SAFEGUARDS

- Apple's iOS operating system support for rapid development of Core ML apps using off-the-shelf devices including wearables, tablets, and handhelds.
  - Potential for highly intuitive and nearly ubiquitous-operator training
  - Accurate and speedy deployment of apps which are highly efficient and very cost-effective
  - Real time or past event analysis of video streams for anomalies that are not pre-determined.
  - Machine learning of normal facility patterns and detection of deviations from it even though everything looks normal
  - Machine learning of signal authentication patterns and detection of deviations (not limited to image processing, for example tracking insider threat with an “always-on” personnel badge)
  - Use of commercial off-the-shelf “Big Data” algorithms and software (e.g. Splunk)
SPLUNK

• What is Splunk (https://www.splunk.com/en_us/homepage.html)
  – The Splunk is a software platform that has the capability to import and index virtually any
    machine data and provide powerful search and analysis features for such data
  – Splunk has its roots in cyber security applications
    • Apps already exist for visualization, analysis & action based on the data stream
    • Add-Ons already exist for optimized data collection.

• What Splunk Isn’t
  – The present Apps and Add-Ons have not been designed to import safeguards data.
  – What constitutes a safeguards significant anomaly in video or other safeguards data stream
    has not been defined.
  – What flags should be placed in the data logs, or the operator’s screen when a safeguards
    relevant anomaly has been detected has not been defined.
CONCLUSION

• Machine language level software tools are now readily available to use artificial language (AI) algorithms

• Apple’s announcement that they will make such tools available in the near future promises ubiquitous access to such tools and the associated software and hardware at a very economical price.

• To utilize these powerful tools for safeguards
  – There needs to be a definition of what constitutes a safeguards significant anomaly in video or other safeguards data stream
  – There needs to be a definition of what flags should be placed in the data logs, or the operator’s screen when a safeguards relevant anomaly has been detected
  – Apps and Add-Ons for various safeguards data streams need to be developed