Friend or Foe: Multi-Modal Military Target Identification

Andrew Jeon • Bassam Halabiya • Naif Ganadily • Zachary Saunders
University of Washington
EE P 567: Machine Learning For Cybersecurity
Professor Radha Poovendran

Introduction & Problem Statement:

War is unpredictable; despite months of planning, steadfast discipline, and constant communication, any fighting force is only the sum of its parts, fallible and imperfect humans. Physical exhaustion, emotional distress, and unfamiliar environments notwithstanding, during combat soldiers are faced with a choice: to shoot a target or not to shoot. Superficially this proposition appears trivial: if the target is an enemy, fire, otherwise do not. However, it is not so. On the modern battlefield, combat occurs from hundreds of yards away, with rifles aimed at soldiers wearing camouflage, belonging to different factions, and organized in guerrilla formations, intentionally designed to challenge target identification. With varying degrees of trickery at play, mistakes do happen. Friendly fire and unnecessary casualties due to mistaken target identification have become a facet of warfare. “Many Americans [are] shocked to learn that 23 percent of all [American] casualties in the Gulf War were from [American] Weapons.” (Shrader) Military engagements can be won or lost by a factor far less than 23%, and therefore should there be a method by which soldiers may positively identify friend from foe, such technology would have a monumental impact on the success of their mission objectives.

Proposed Solution:

After reviewing military processes and combat training methodologies, we believe that the most apt opportunity to perform target identification is when a rifle is aimed at an enemy. Standard-issue combat equipment contains a variety of active rifle optics that perform thermal imaging, night vision, and other computational tasks. We propose that these existing optic systems be retrofitted with a machine learning model that performs camouflage recognition that aids the soldier in making their snap decision. Although such a technology, once deployed, will alone empower soldiers to make more informed decisions, per Kerckhoff’s principle, the foundational cybersecurity concept that states “the security of a cryptosystem must lie in the choice of its keys only; everything else (including the algorithm itself) should be considered public knowledge.” (Petitcolas), we must account for the fact that the enemy force is not only aware that such a system has been deployed, but they also have all necessary knowledge in what features the model uses as a basis for classification. With this information in hand, it would then be possible for the enemy to change their uniform to confuse our model and not only disable the effectiveness of the tool but even turn the tool against the operator by incorrectly labeling enemy forces as friendly.

With this consideration in mind, we will also provide the soldier with a secondary authentication method. Attached to the soldier's firearm will be an added piece of equipment, a directional antenna, and a software-defined radio (SDR). Additionally, all soldiers’ uniforms will be equipped with embedded radio receivers & transponders. Much like an optic system, the antenna and SDR will point at a target in a plane with the firearm. When aimed at a target, the SDR will issue a challenge radio signal towards the direction of the target. If aimed at a friendly, the transponder will hear the signal and provide a response, confirming that they are indeed friendly. By adding this second factor, the holistic system will become far more accurate and less susceptible to abuse.

Training & Evaluation Dataset:

We will be compiling our own training and evaluation dataset composed of 1000 images sourced from the internet. In an effort to enhance the accuracy of our model, we will be limiting the scope of our data to two categories and eight subcategories. Of the 1000 total images, 500 will be that of the American military and 500 of the Russian military, with each set of 500 further divided into subsets for the four major branches: army, navy, air force, and marines (1000 total / 2 forces = 500 / 4 branches = 125 per branch per force). While the US military has these 4 branches, Russia lacks a formal Marine corps, for this comparison alone we will be comparing the US marine corps to images from the Russian Army. These 1100 images will then be preprocessed and augmented by Roboflow with each image duplicated with varying degrees of noise, rotation, and other visual effects. After applying data augmentation techniques, we anticipate the modified dataset to enlarge to 4000+ images.Furthermore, in addition to the military faction samples, we supplement the dataset with null examples, roughly 10% of the entire dataset size, to allow our ML model to learn what does and does not constitute as one of the two main classes (i.e. friend or foe). For our purposes, American forces will represent the friendly force and Russian forces will be the enemy. With that said, however, we will take care to design the model such that it is adaptable to multiple enemy and friendly forces, should you train it accordingly.

Next Milestone:

By the next milestone, we expect to have our dataset manually labeled and ingested into the tool Roboflow. Roboflow allows us to build a larger dataset collaboratively and asynchronously, and then expose our dataset to our model. Regarding the model itself, we expect to have the architectural considerations complete, some degree of code written, and a version of our model trained, validated, and deployed on Roboflow Similarly, we plan to have early revisions of the challenge/response system drafted, albeit not yet feature complete, particularly how to apply Kerckhoff's principle to the SDR to transponder paradigm.

References:

Petitcolas, F.A.P. (2023). Kerckhoffs' Principle. In: Jajodia, S., Samarati, P., Yung, M. (eds) Encyclopedia of Cryptography, Security and Privacy. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-27739-9_487-2

Shrader, C. R. (n.d.). *The US Army War College Quarterly: Parameters*. The US Army War College Quarterly: Parameters The US Army War College Quarterly: Parameters. https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1645&context=parameters