**CHARACTERIZING AND EVALUATING ADVERSARIAL EXAMPLES**

**FOR OFFLINE HANDWRITTEN SIGNATURE VERIFICATION**

**ABSTRACT**

The phenomenon of Adversarial Examples is attracting increasing interest from the Machine Learning community, due to its significant impact to the security of Machine Learning systems. Adversarial examples are similar (from a perceptual notion of similarity) to samples from the data distribution, that “fool” a machine learning classifier. For computer vision applications, these are images with carefully crafted but almost imperceptible changes, which are misclassified. In this work, we characterize this phenomenon under an existing taxonomy of threats to biometric systems, in particular identifying new attacks for Offline Handwritten Signature Verification systems. We conducted an extensive set of experiments on four widely used datasets: MCYT-75, CEDAR, GPDS-160 and the Brazilian PUC-PR, considering both a CNN-based system and a system using a handcrafted feature extractor (CLBP). We found that attacks that aim to get a genuine signature rejected are easy to generate, even in a limited knowledge scenario, where the attacker does not have access to the trained classifier nor the signatures used for training. Attacks that get a forgery to be accepted are harder to produce, and often require a higher level of noise - in most cases, no longer “imperceptible” as previous findings in object recognition. We also evaluated the impact of two countermeasures on the success rate of the attacks and the amount of noise required for generating successful attacks.

**PROPOSED SYSTEM**

In this paper we investigated the impact of adversarial examples on biometric systems, in particular by identifying threats to Offline Handwritten Signature Verification under the point of view of Adversarial Machine Learning. The first point of attack (#1) in a biometric system is the user interface that collects the sample (e.g. a scanner capturing a document with a signature, or a mobile application taking a picture of a bank cheque). For many biometrics, attacks on this first point mainly consist of spoofing attacks that normally use a fabricated fake biometric trait. Possible defenses for such attacks rely on liveness detection. On the signature verification task, simulated and traced forgeries can be considered attacks targeting this stage. A second set of attack points refer to attacks in the communication between different components of the system (#2, #4) (for example, intercepting and replacing the sensor input or the extracted features, that is input to the subsequent module). Defenses for such attacks involve encrypting the communication between the different modules. The software modules (#1, #3, #5, #6, #7) may present vulnerabilities in the code (such as buffer overflow) that can be exploited by a malicious user. The classifier training (#5) can be targeted for poisoning attacks (e.g. adding samples from another user in the training data for subsequent intrusion). For adaptive systems, the template update rule (#7) can be targeted to update the template database (e.g. for intrusion).

**PROPOSED SYSTEM ADVANTAGES**

* Security.
* Transferability is greatly reduced
* Success rate of attacks has been reduced

**PROPOSED SYSTEM BLOCK DIAGRAM**

Adaptive update

Classifier training

Feature extraction

Training dataset

Verification

Feature extraction

Sensor

New sample

Output

**FIG 1.1: DETAILED BLOCK DIAGRAM OF PROPOSED SYSTEM**

**Hardware Requirements**

The necessary hardware regarding private PC that comprises configuration as specified as follows:-

1. Processor: Intel core i3/i5.

2. Disk capability: 1GB for MATLAB only.

3. RAM: 2GB.

**Software Tool used**

The necessary program regarding private PC that comprises configuration as specified as follows:-

1. Windows 7(64-bit) operating system.

2. MATLAB version R2012a.

**Image Processing Toolbox**

Image processing device box permits carrying out image improvement, deblurring of image, characteristic identification, decreasing of noise, image segmentation, arithmetical alteration, as well as registration of image. Image processing device intended for the execution regarding methods proposed are specified below:-

1. Fundamental import as well as export

2. Display

**Features of MATLAB**

* Interactive background meant for aim investigation as well as resolving the difficulty.
* MATLAB is a sophisticated language intended for creating, calculating as well as building up a purpose.
* It contains numerical tasks such as figures, calculus, sorting out, developments, mathematical integration, as well as working out equations.
* Graphics integrated intended for visualization.
* Intended for generating traditional plot integrated equipments is accessible.
* Troubles as well as way outs are given in well-known numerical symbol.