

IS THERE ANYTHING LEFT TO SAY ? (PERHAPS THAT WE ACHIEVED THE GOAL ? mentioning the article ?)

תוצאות ו/או תמונות מתקיפות (כדאי להכניס גם collage מסויים ?)

תוצאות ו/או תמונות מתקיפות (כדאי להכניס גם collage מסויים ?)

Figure 1

The architecture of an encrypting model (fashion-mnist)

**Attacking**

Attacking the sufficiently accurate models . (e.g. Models that apply permutation or AES in CTR mode of operration) Figure 2 …

**"Building”**

Training models on encrypted images , on the datasets Mnist and Fashion-Mnist.

Encryption techniques (See figure 1) :

* Permutation (on the pixels)
* AES in ECB,CBC and CTR modes of operation

EXAMPLES OR RESULTS

**בס"ד**

FINAL RESULTS TABLE OR DISTRIBUTED TABLES ?

FUTURE WORK

* Padding
* CARLINI ?
* ECB ?

**LOOK AT THIS STEVE :**

**Vision :**

**BLOCK -> RESULT OR EXAMPLE**

GOALS

**סמל של מרכז הסייבר**

**Problem Description**

Building DNN models with high accuracy level which are sufficiently resistant to adversarial examples (attack)

DEFENCE AGAINST

ADVERSARIAL EXAMPLES

Yishay Asher, Steve Gutfreund

Instructor: Hanan Rosemarin

