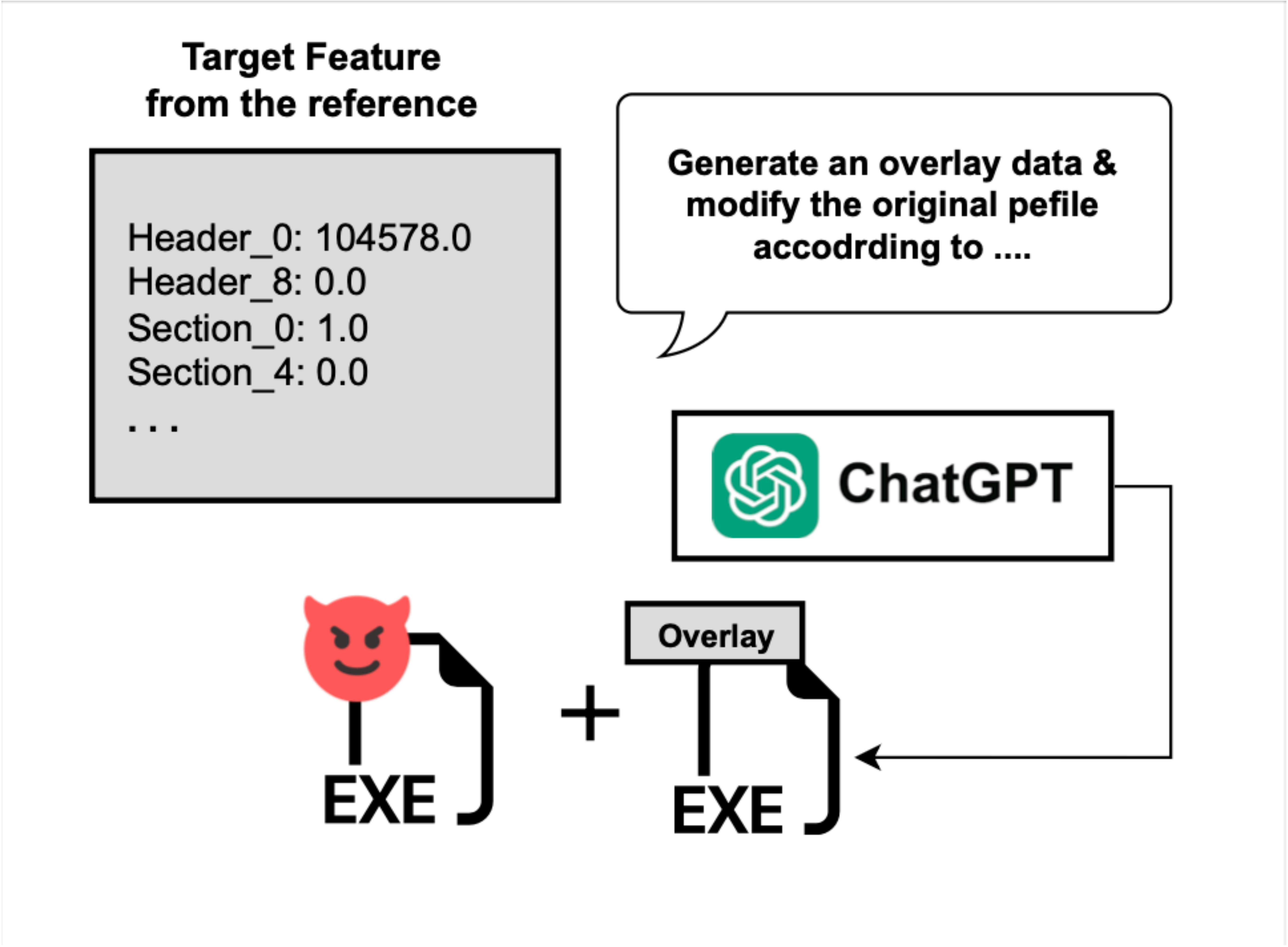
Saeyeon Hong

👨‍🔬 I am a master's student at AISEC at Ewha Womans University, where I am advised by Prof. Se Eun Oh.

📫 Contact: saeyeonhong@ewha.ac.kr or connect with me on LinkedIn.

💡 My research leverages machine learning and deep learning techniques to address problems in security. I have worked on Membership Inference Attacks in text-to-speech diffusion models. I have also explored the use of Large Language Models (LLMs) in security-related applications, such as LLM-based malware generation. Broadly, I'm interested in the intersection of AI and other domains — using AI to solve real-world problems in areas like security, healthcare, and beyond. ☕ Feel free to reach out — I'm always open to interesting discussions and collaborations.

Weapon-LLM



Target Feature
from the reference

```
Header_0: 104578.0
Header_8: 0.0
Section_0: 1.0
Section_4: 0.0
. . .
```

Generate an overlay data & modify the original pefile accodrding to ....

Weapon-LLM

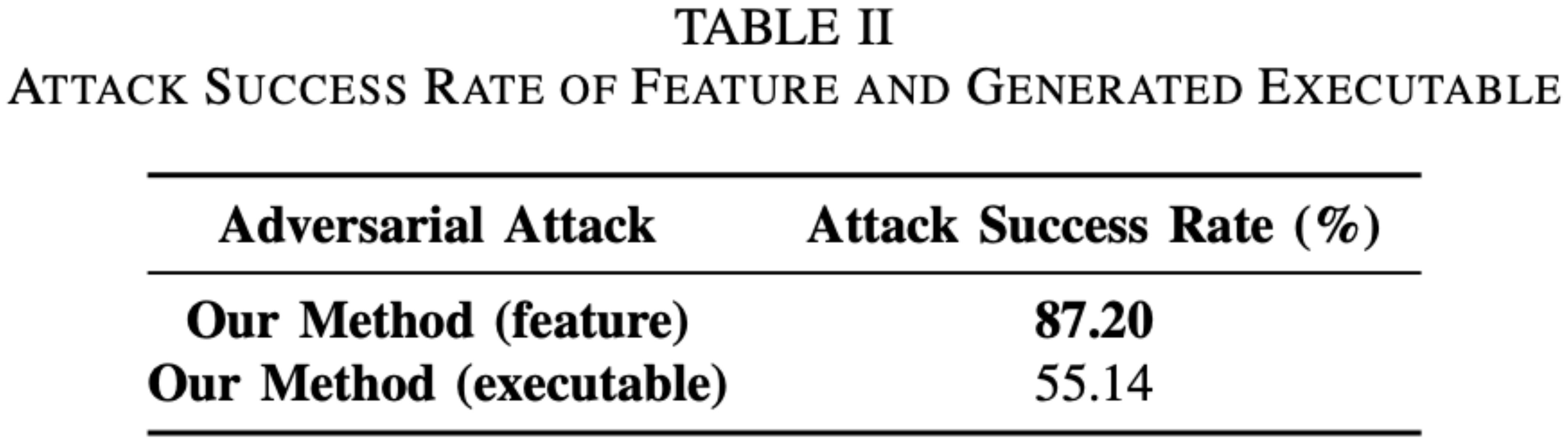
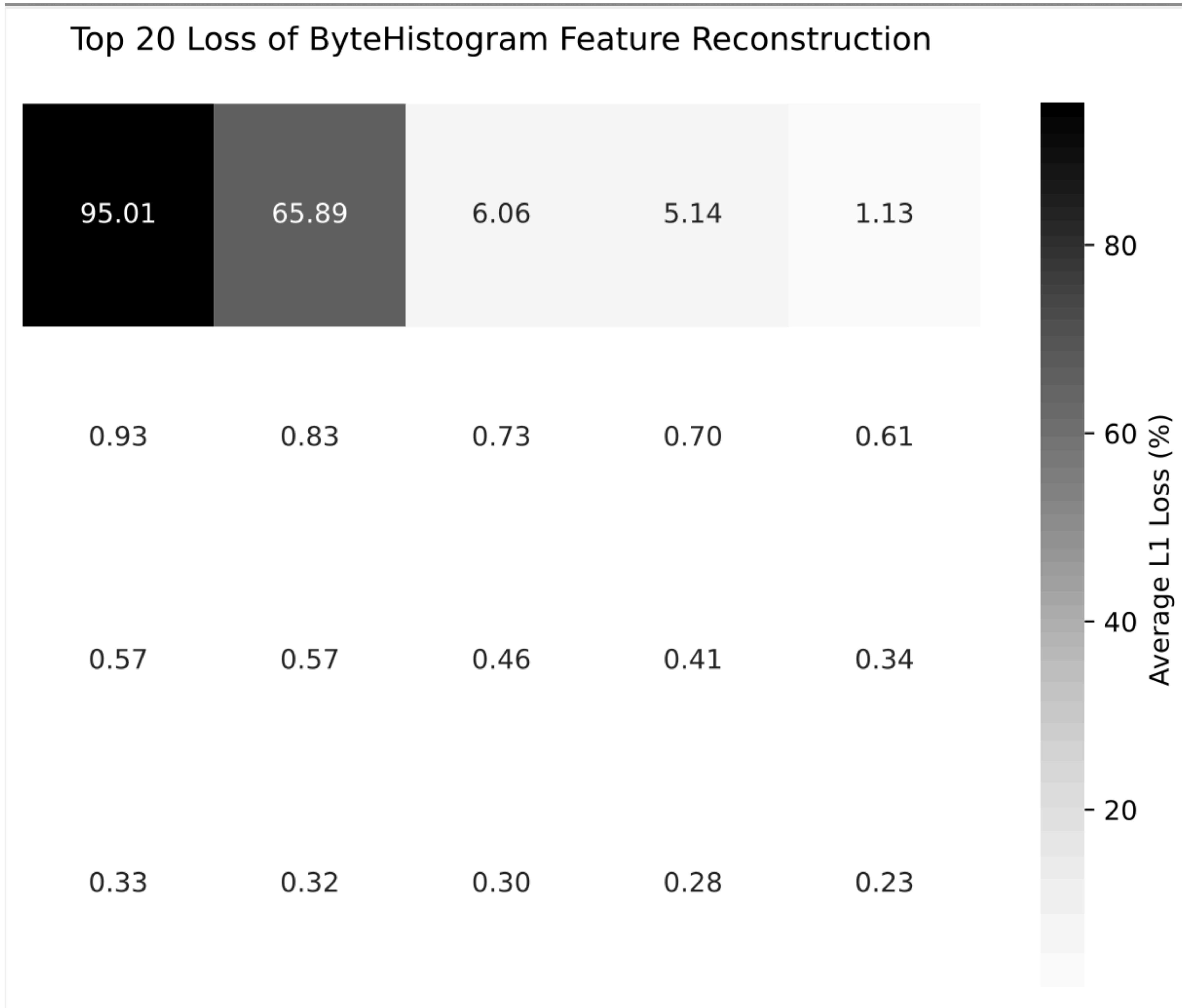


TABLE II
ATTACK SUCCESS RATE OF FEATURE AND GENERATED EXECUTABLE

Adversarial Attack	Attack Success Rate (%)
Our Method (feature)	**87.20**
Our Method (executable)	55.14



Top 20 Loss of ByteHistogram Feature Reconstruction