Letter of Correction to paper "Enhancing Boundary Attack in Adversarial Image Using Square Random Constraint" by Tran Van Sang et al. (2022)

Tran Van Sang[1]
4040961653@g.ecc.u-tokyo.ac.jp

Tran Phuong Thao [1]
tpthao@yamagula.ic.i.u-tokyo.ac.jp

Rie Shigetomi Yamaguchi [1]
yamaguchi.rie@i.u-tokyo.ac.jp

Toshiyuki Nakata [1]
nakata.toshiyuki@sict.i.u-tokyo.ac.jp

In the paper "Enhancing Boundary Attack in Adversarial Image Using Square Random Constraint" by Tran Van Sang, Tran Phuong Thao, Shigetomi Rie Yamaguchi, and Toshiyuki Nakata, 2022 Proceedings of the 2021 ACM Workshop on Security and Privacy Analytics (IWSPA), Association for Computing Machinery, 2022, doi: 10.1145/3510548.3519373, there was an error in the second paragraph in Subsection 5.1 Accuracy and Running Time.

In this paragraph, we refer to the incorrect figure (Figure 5), and the explanation of the referred figure is inexact. At the end of this paragraph, we conclude that the proposed method can generate stronger adversarial images that look almost exactly like the original target images (while the original Boundary Attack method does not). However, the experiments' results in this paper do not fully support this statement.

The readers should omit this paragraph when they read the paper. Nonetheless, this omission does not affect the correctness of numerical results and also the rest of the paper.

[1]The University of Tokyo, Bunkyo, Tokyo, Japan