Outlook

WISE-2024 notification for paper 368

From WISE-2024 <wise2024-0@easychair.org>
Date Tue 9/3/2024 1:58 PM
To Tamer Ahmed Eltaras <tamer.ahmedeltaras@polito.it>

Dear Tamer Ahmed Eltaras

We are glad to inform you that your paper "368 - R-CONV: An Analytical Approach for Efficient Data Reconstruction via Convolutional Gradients" has been accepted for presentation at the WISE 2024 conference. Congratulations!

368 - R-CONV: An Analytical Approach for Efficient Data Reconstruction via Convolutional Gradients

We received 335 submissions this year. Due to space limitations, we were only able to accept 110 high-quality research papers.

Your paper is limited to (15) pages. We will send you shortly the camera-ready preparation steps.

In the meanwhile, please visit the conference webpage and register. Please note that, it is compulsory to pay at least one author registration per paper in order for the paper to be included in the conference proceedings and presented at the conference.

We take the occasion to inform you that WISE 2024 has 3 co-located workshops, a PhD symposium and a DEMO track and submission is still open: https://wise2024-qatar.com/

Best regards,

WISE-2024 Program Committee Co-Chairs

SUBMISSION: 368
TITLE: R-CONV: An Analytical Approach for Efficient Data Reconstruction via Convolutional Gradients

---------- REVIEW 1 ----------
SUBMISSION: 368
TITLE: R-CONV: An Analytical Approach for Efficient Data Reconstruction via Convolutional Gradients
AUTHORS: Tamer Ahmed Eltaras, Qutaibah Malluhi, Alessandro Savino, Stefano Di Carlo and Adnan Qayyum

---------- Overall evaluation ----------
SCORE: 1 (Weak accept (Indicative Meaning: The paper addresses an interesting problem. The proposed solution seems to be valid. The paper has some weaknesses that can be addressed without the need to rethink the whole solution.))
----- TEXT:
The paper introduces a novel method for reconstructing training data by exploiting gradients, demonstrating the attack even in the presence of non-invertible activation functions. The research problem is interesting and relevant.

The paper can be improved as follows. The mathematical terms in the paper are not easy to follow. The experiments could be enhanced by showing how the attacks perform on more complex networks.

---------- REVIEW 2 ----------
SUBMISSION: 368
TITLE: R-CONV: An Analytical Approach for Efficient Data Reconstruction via Convolutional Gradients
AUTHORS: Tamer Ahmed Eltaras, Qutaibah Malluhi, Alessandro Savino, Stefano Di Carlo and Adnan Qayyum

---------- Overall evaluation ----------
SCORE: 1 (Weak accept (Indicative Meaning: The paper addresses an interesting problem. The proposed solution seems to be valid. The paper has some weaknesses that can be addressed without the need to rethink the whole solution.))
----- TEXT:
This paper introduces R-CONV, an analytical attack that primarily exploits convolutional gradients. It addresses the challenge that forward convolution constraints are not fully applicable for non-invertible activation functions by demonstrating that gradient constraints for common activation functions can still be computed. This is achieved by expressing the derivative of the activation in terms of its outputs instead of the inputs. The authors showcase the effectiveness of R-CONV through experiments that successfully invert convolutional neural networks with ReLU activation functions. The results, compared to those of R-GAP and DLG, highlight the improved performance of R-CONV.

Strengths:

The paper presents a novel method that extends analytical gradient inversion attacks.

It shows a way to reconstruct the input in the presence of non-invertible functions, which is a significant extension of existing work.

It compares the performance with two well-known methods in the literature, R-GAP and DLG.

The authors provide open-source code for their implementation, ensuring reproducibility.

The paper features a detailed experimental section that compares R-CONV with top methods like DLG and R-GAP. Using datasets CIFAR-10, CIFAR-100, and MNIST, along with various CNN architectures, it shows that R-CONV excels in reconstruction quality and efficiency.

Weaknesses:

The results presented in the paper consider only a batch size of one training example, and do not demonstrate the effectiveness of the method on batch sizes greater than one.

---------- REVIEW 3 ----------
SUBMISSION: 368
TITLE: R-CONV: An Analytical Approach for Efficient Data Reconstruction via Convolutional Gradients
AUTHORS: Tamer Ahmed Eltaras, Qutaibah Malluhi, Alessandro Savino, Stefano Di Carlo and Adnan Qayyum

---------- Overall evaluation ----------
SCORE: 2 (Accept (Indicative Meaning: The paper addresses an important problem. The proposed solution is original and valid. The paper has some minor issues that can be easily fixed.))
----- TEXT:
The paper tackles an interesting and timely problem. The mathematical foundations of the solution are well explained and detailed. However, reading the paper was daunting because of the lack of examples. The paper should be improved with respect to that aspect.