REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
22-10-2021	Final Report	2-Jul-2018 - 1-Sep-2021

4. TITLE AND SUBTITLE
Final Report: New Approaches to Combine Individual Training Losses for Machine Learning

5a. CONTRACT NUMBER
W911NF-18-1-0297

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
State University of New York (SUNY) at Al
Office for Sponsored Programs, MSC 312
1400 Washington Avenue
Albany, NY 12222 -0100

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
73042-CS.3

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chang Ming-Ching
UU	UU	UU	UU		19b. TELEPHONE NUMBER 000-000-0000

RPPR Final Report
as of 26-Jan-2022

Agency Code: 21XD

Proposal Number: 73042CS **Agreement Number: W911NF-18-1-0297**
INVESTIGATOR(S):

Name: Chang Ming-Ching
Email: mchang2@albany.edu
Phone Number: 0000000000
Principal: Y

Organization: **State University of New York (SUNY) at Albany**
Address: Office for Sponsored Programs, MSC 312, Albany, NY 122220100
Country: USA
DUNS Number: 152652822 EIN:
Report Date: 01-Dec-2021 Date Received: 22-Oct-2021
Final Report for Period Beginning 02-Jul-2018 and Ending 01-Sep-2021
Title: New Approaches to Combine Individual Training Losses for Machine Learning
Begin Performance Period: 02-Jul-2018 **End Performance Period:** 01-Sep-2021
Report Term: 0-Other
Submitted By: Siwei Lyu Email: siweilyu@buffalo.edu
Phone: (518) 437-4938

STEM Degrees: 3 **STEM Participants:**

Major Goals: The proposed work will focus on several fundamental research questions concerning the aggregate loss: are there any other types of aggregate loss beyond the average individual losses?; if so, what will be a general abstract formulation of these new aggregate loss?; how can the new aggregate losses be adapted to different machine learning problems?; and what are the statistical and computational behaviors of machine learning algorithms using the general aggregate losses?. Pursuing answers to these questions, we conduct the proposed project in four interrelated thrusts. 1. Rank-based aggregate losses for binary classification. Building upon our recent work, we explore new types of rank-based aggregate losses for binary classification and study efficient algorithms optimizing learning objectives formed based upon them. 2. Theoretical analysis of rank-based aggregate losses. To deepen our understanding of the binary classification algorithms developed using the rank-based aggregate losses, we will study their asymptotic behaviors such as generalization and consistency. 3. Rank-based aggregate losses for other learning problems. The ranking based aggregate losses will be extended to other supervised problems (multi-class and multi-label learning and supervised metric learning) and unsupervised learning. 4. General properties and new types of aggregate losses. An aggregate loss will be abstracted as a set function that maps the ensemble of individual losses to a number. This abstraction will be exploited to study the general properties and propose new forms of aggregate losses.

Accomplishments: There are three major activities we have conducted during the reported period.

(1) First, continuing our work reported in the last period, we have furthered our studies on a new aggregate loss type known as the average of ranked range (AoRR). We specifically studied the generalization of learning algorithms based on AoRR loss, and investigated different approaches to choose hyper-parameters in the learning algorithm. ?

(2) Based on the ranking based learning objectives, we develop methods to create adversarial perturbations that can be used to attack top-k multi-label learning-based image annotation systems. Our methods explicitly consider the top-k ranking relation and are based on novel loss functions.?

(3) The new aggregate loss has also been applied to the Computer vision problem of human pose estimation, where to train a deep neural network with many layers we apply the top-k loss to improve its robustness.

Specific objectives:

For the theoretical research on the aggregate loss, our goal is to set up connections with distributional robust

training and adversarial robust training, which are alternative learning methodologies aiming to adapt to biased training data and robust to adversarial examples. For application of new aggregate loss to the deep correlated predictive subspace learning, we investigate the use of top-k like loss in the presence of missing data views. We also aim to use new types of aggregate losses to study the vulnerabilities of current top-k multi-label learning algorithms. For pose estimation, the idea of using the average of the top-k performer has been used empirically but we want to use the new aggregate loss in a principled way to unify existing methods.

Significant results, including major findings, developments, or conclusions (both positive and negative)

We developed adversarial attack algorithms for top-k multi-label (TkML) learning based on a continuous formulation of the ranking operation. Specifically, we note that to perturb the predictions of a TkML algorithm, it is sufficient to clear any ground-truth labels from the top-k set. There are many different ways to achieve this, but we will focus on ones that enlist the ``least actions'', i.e., perturbing the predicted labels with minimum changes to the original label rankings. Our algorithm thus finds such changes and it helps to expose the vulnerabilities of such algorithms in applications. This work is currently in submission to the IEEE International Conference on Computer Vision, 2021. Furthermore, we describe a combination loss of
rank-based aggregate losses and individual losses as a new learning objective for improving the robustness of multi-label learning in the face of outliers in sample and labels alike. Our empirical results highlight the effectiveness of the proposed optimization frameworks and demonstrate the applicability of proposed losses using synthetic and real data sets. This work is currently in submission to Journal of Machine Learning Research, 2021.

Key outcomes or other achievements.

During the reported period, with the provided fund, we have published several papers in related research areas of machine learning and computer vision. Here is a list of papers we have published or currently in submission.

[1] S. Hu, Y. Ying, X. Wang, and S. Lyu, “Learning by minimizing the sum of ranked range,” in Advances in Neural Information Processing Systems (NeurIPS), (Montreal, QC, Canada), 2020.
[2] S. Hu, Y. Ying, X. Wang, and S. Lyu, “Sum of Ranked Range Loss for Supervised Learning”, in submission to Journal of Machine Learning Research, 2021.
[3] S. Hu, L. Ke, X. Wang, and S. Lyu, “Adversarial Attacks to Top-k Multi-Label Learning”, in submission to IEEE International Conference on Computer Vision, 2021.
[4] L. Ke, M. Chang, J. Shieh, and S. Lyu“DSPnet: A Unified Network for PersonDetection, Instance Segmentation and PoseEstimation”, in submission to British Machine Vision Conference, 2021.

Training Opportunities: Two Ph.D. students (Shu Hu and Ehab Albawdawy) are partially supported by the project. The project provides supports for them to work as research assistants mentored by the PI. Through this collaboration experience, they have gained skills in experimental design, code writing and mathematical formulation, as well as paper writing and presentation.

Results Dissemination: The research results are disseminated to the research community through publications in conferences and journals. The list of publications are given in the Accomplishments section.

Honors and Awards: IEEE Region 1 Technological Innovation (Academic) Award (2021).

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Siwei Lyu
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

RPPR Final Report
as of 26-Jan-2022

Participant Type: Graduate Student (research assistant)
Participant: Shu Hu
Person Months Worked: 9.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Ehab Albadaway
Person Months Worked: 9.00 **Funding Support:**
Project Contribution:
National Academy Member: N

ARTICLES:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transaction on Pattern Analysis and Machine Intelligence
Publication Identifier Type: Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 6/30/20 12:00AM Date Published:
Publication Location:
Article Title: Average top-k loss for supervised learning
Authors: S. Lyu, Y. Fan, Y. Ying, and B. Hu
Keywords: Machine Learning, Aggregate Loss
Abstract: Learning objective is a fundamental component in any machine learning problem. In forming learning objectives, we often need to aggregate a set of individual values to a single numerical value. Such cases occur in the aggregate loss, which combines individual losses of a learning model over each training sample, and in the individual loss for multi-label learning, which combines prediction scores over all class labels.
Distribution Statement: 3-Distribution authorized to U.S. Government Agencies and their contractors
Acknowledged Federal Support: **Y**

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: 2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)
Date Received: 22-Oct-2021 Conference Date: 24-Oct-2020 Date Published:
Conference Location: Las Vegas, NV, USA
Paper Title: Explainable and Efficient Sequential Correlation Network for 3D Single Person Concurrent Activity Detection
Authors: Yi Wei, Wenbo Li, Ming-Ching Chang, Hongxia Jin and Siwei Lyu
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 26-Jan-2022

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Siwei Lyu
Signature Date: 10/22/21 9:19PM

Ming-Ching Chang
University at Albany, State University at New York
New Approaches to Combine Individual Training Losses for Machine Learning
Proposal 73042-CS
Contract #W911NF-18-1-0297

Objective

The proposed work aims to answer the following questions:

- what will be a general abstract formulation of these new aggregate losses?
- how can the new aggregate losses be adapted to different machine learning problems?
- and what are the statistical and computational behaviors of machine learning algorithms using the general aggregate losses?

Approach

The proposed work will study the aggregate loss from a general theoretical perspective and develop new types of aggregate losses for various machine learning problems, efficient algorithms optimizing the new aggregate losses and statistical analysis of such algorithms.

Accomplishments

- Our work on the theoretical study of new types of aggregate losses has led to several high quality scientific publications in prestigious machine learning conferences (NeurIPS), and journals (IEEE T-PAMI).
- Applications of the rank-based aggregate losses have led to significant performance improvement to practical problems including detecting AI-synthesized media and human pose estimation.

Conclusions

- Our research has shown that the study of aggregate loss is important to improve the overall understanding and design of machine learning algorithms.
- The incorporation of new types of aggregate losses in practical applications demonstrates their effectiveness.

Scientific Barriers

- This research is motivated by the current lack of comprehensive and systematic study of its theory and practical applications.
- The critical gap that is addressed by this research is the deeper of the aggregate losses and their roles in machine learning algorithms.

Significance

- As the link between the training data and the model to be learned, the aggregate loss is a fundamental component in machine learning algorithms.
- This research vertically advances the field because it provides new set of algorithms based on the new aggregate loss types.
- This research is transformative because this research provides a previously unexplored point of view to machine learning. methods.

Collaborations, Partnerships, and Leveraged Funding

- During the period of this project, the application domain of the research topic, i.e., new types of aggregate losses, is chosen to be in the area of computer vision and digital media forensics
- We seek collaboration with GE Global Research Center, and the DARPA through the DARPA MediFor program.

Future Plans

Our preliminary study of aggregate losses has led to fruitful research, and in the future we aim to further extend this work

- We would like to further deepen our understanding of the theoretical aspect of the new aggregate losses, in particular, their asymptotic behaviors
- We will further study more flexible types of nonlinear, non-decomposable aggregate losses could be designed based on the combination of individual scores

Proposal 12345-AB
Contract #W911NF-YY-X-1234

Technology Transfer

This work itself so far has not led to any technology transfer yet. But our work on detecting AI-synthesized audios and videos, which incorporates the new types of aggregate losses and supported by the DARPA MediFor program, is being transferred to DARPA and US Secrete Service.

Awards, Publications, and full-time equivalents

- Google Faculty Research Award (2019): for research on detecting AI-synthesized media
    - Relevance to the ARO project: an important component in the proposed method is the novel learning objectives
- Publications in the past fiscal year
    1. S. Hu, Y. Ying, X. Wang, and S. Lyu, “Learning by minimizing the sum of ranked range,” in Advances in Neural Information Processing Systems (NeurIPS), (Montreal, QC, Canada), 2020.
    2. S. Lyu, Y. Fan, Y. Ying, and B. Hu, “Average top-k loss for supervised learning,” IEEE Transactions on Pattern Analysis and Machine Intelligence, (accepted), 2020.
    3. Y. Fan, B. Wu, R. He, B. Hu, Y. Zhang, and S. Lyu, “Group-wise ranking loss for multi-label learning,” IEEE Access, vol. to appear, 2020.
    4. E. AlBadawy and S. Lyu, “Voice conversion using speech-to-speech neuro-style transfer,” in Interspeech, (Shanghai, China), October 2020.
- Full-time equivalents
    1. Shu Hu, graduate student, 50% support
    2. Ehab Albadaway, graduate student, 33.3% support
    3. Daniel Tian, High school student volunteer, no financial support
    4. Yanbo Fan, visiting student, no financial support