Mingyuan BAI, Derun ZHOU, Qibin ZHAO, 2024. TendiffPure: a convolutional tensor-train denoising diffusion model for purification. *Frontiers of Information Technology & Electronic Engineering*, 25(1):160-169. https://doi.org/10.1631/FITEE.2300392

TendiffPure: a convolutional tensor-train denoising diffusion model for purification

Key words: Diffusion models; Tensor decomposition; Image denoising

Corresponding author: Qibin ZHAO
E-mail: qibin.zhao@riken.jp
ORCID: https://orcid.org/0000-0002-4442-3182

Motivation

1. Diffusion models are recently renowned for their powerfulness on data generation.

2. Because of their stochastic differential equation (SDE) nature, diffusion models requires a large number of steps to generate data and has low sample efficiency. Existing methods are based on knowledge distillation which enhances the efficiency at the cost of performance.

3. Tensor decomposition and tensor networks are effective method for model compression.

Method

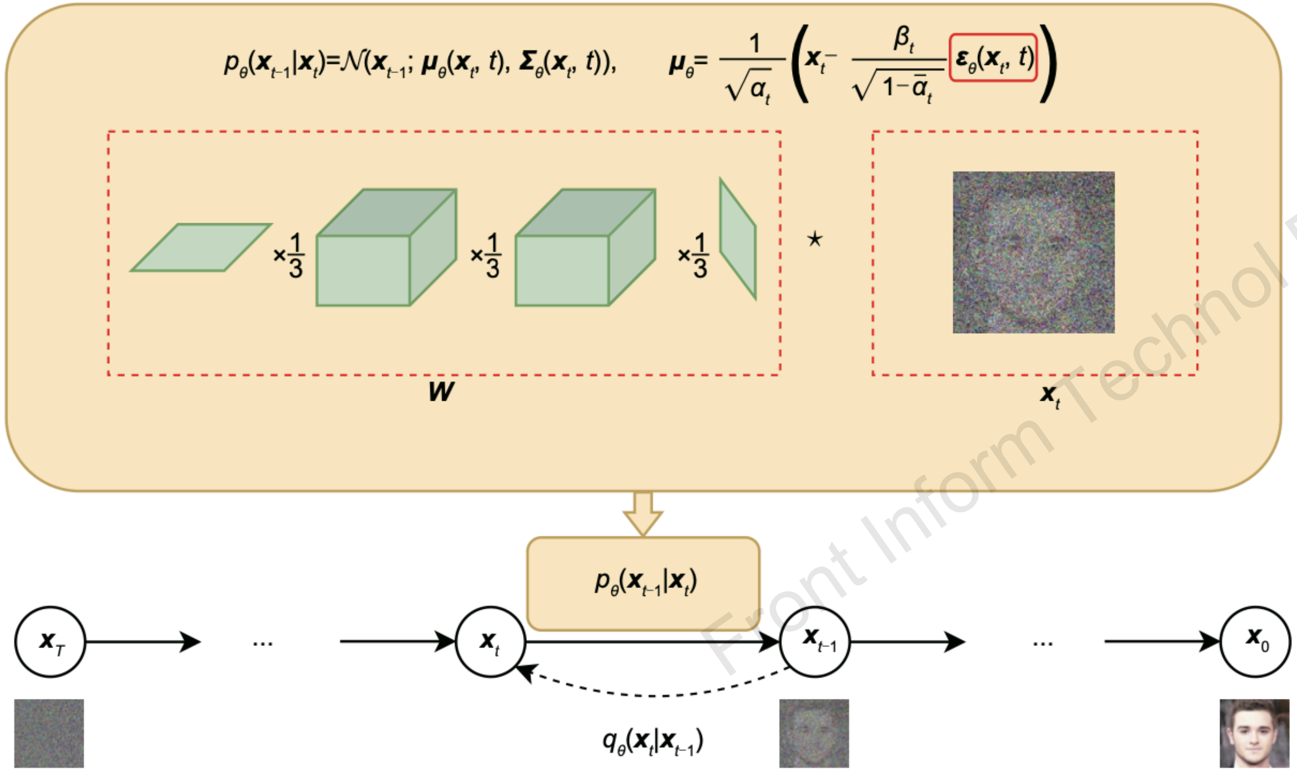

Fig. 1 A brief summary of TendiffPure

Based on tensor-train decomposition, we compress parameters of the backbones of diffusion models for purification and propose TendiffPure.

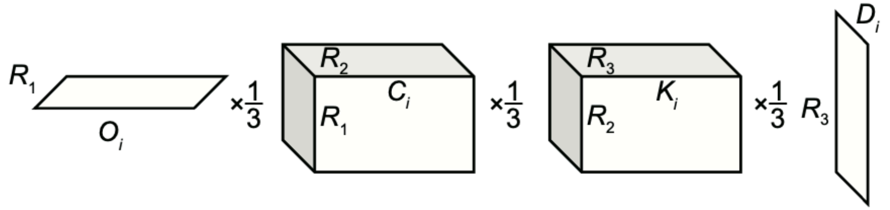

Fig. 2 Convolution tensor-train kernels of TendiffPure

Experiments

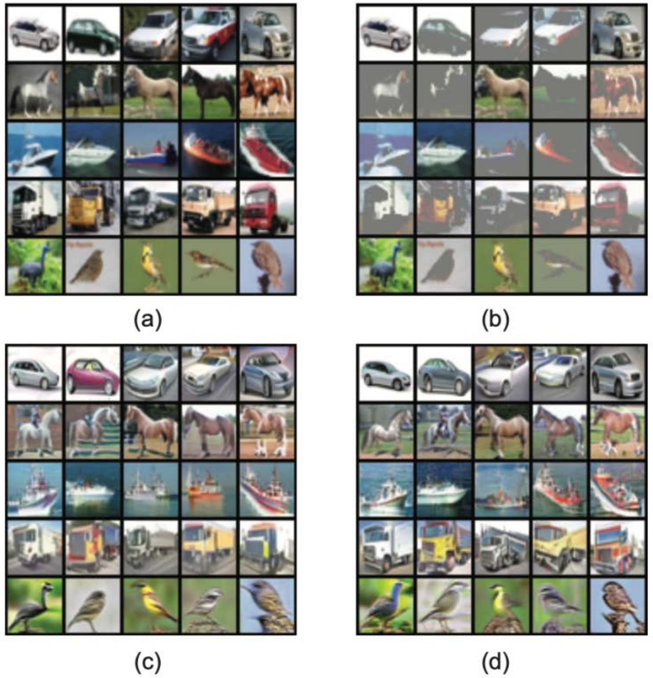

Fig. 5 Selected purified or denoised images by TendiffPure on the CIFAR-10 dataset with AutoAttack compared with DDPM (DiffPure): (a) original images; (b) AutoAttacked; (c) DDPM (DiffPure); (d) TendiffPure

Table 1 Purification performance of TendiffPure on CIFAR-10 evaluated by the pre-trained ResNet56 classifier

Model	Standard accuracy (%)	Robust accuracy (%)		
		Gaussian noise	Salt and pepper noise	AutoAttack
DDPM	93.34 ± 0.13	93.39 ± 0.34	92.89 ± 0.66	91.31 ± 0.44
DDIM	54.41 ± 0.39	54.85 ± 0.40	37.83 ± 0.25	44.86 ± 0.31
TendiffPure (ours)	$\mathbf{95.62 \pm 0.30}$	$\mathbf{95.02 \pm 0.47}$	$\mathbf{95.65 \pm 0.17}$	$\mathbf{92.45 \pm 0.24}$

Best results are in bold

Table 4 Ablation studies of TendiffPure on CIFAR-10 evaluated by the pre-trained ResNet56 classifier

Rank	Standard accuracy (%)	Robust accuracy (%)		
		Gaussian noise	Salt and pepper noise	AutoAttack
$(3,3,3)$	50.42 ± 0.36	50.97 ± 0.17	49.56 ± 0.18	46.01 ± 0.38
$(4,4,4)$	67.45 ± 0.08	67.76 ± 0.16	64.60 ± 0.62	57.82 ± 0.47
$(4,3,4)$	63.74 ± 0.29	61.51 ± 0.61	65.20 ± 0.44	58.33 ± 0.30
$(4,4)$	93.11 ± 0.57	94.04 ± 0.32	94.89 ± 0.24	$\mathbf{92.45 \pm 0.24}$
$(3,3)$	92.56 ± 0.66	91.36 ± 0.37	91.80 ± 0.29	91.31 ± 0.24
$(3,4)$	$\mathbf{95.62 \pm 0.30}$	$\mathbf{95.02 \pm 0.47}$	$\mathbf{95.65 \pm 0.17}$	91.03 ± 0.37
$(2,3)$	91.71 ± 0.22	91.54 ± 0.25	91.36 ± 0.42	90.02 ± 0.57
(2)	92.66 ± 0.17	92.99 ± 0.38	91.65 ± 0.51	90.87 ± 0.40

Best results are in bold

Experiments

Table 2 Purification performance of TendiffPure on Fashion-MNIST evaluated by the pre-trained LeNet classifier

Model	Standard accuracy (%)	Robust accuracy (%)		
		Gaussian noise	Salt and pepper noise	AutoAttack
DDPM	93.69 ± 0.15	92.79 ± 0.34	92.38 ± 0.30	90.72 ± 0.39
DDIM	69.60 ± 0.24	47.75 ± 0.42	66.65 ± 0.37	68.86 ± 0.36
TendiffPure (ours)	$\mathbf{95.64 \pm 0.32}$	$\mathbf{93.62 \pm 0.06}$	$\mathbf{94.82 \pm 0.36}$	$\mathbf{92.43 \pm 0.22}$

Best results are in bold

Table 5 Ablation studies of TendiffPure on Fashion-MNIST evaluated by the pre-trained LeNet classifier

Rank	Standard accuracy (%)	Robust accuracy (%)		
		Gaussian noise	Salt and pepper noise	AutoAttack
$(3,3,3)$	57.99 ± 0.08	41.34 ± 0.34	37.78 ± 0.42	55.71 ± 0.35
$(4,4,4)$	82.32 ± 0.61	66.83 ± 0.44	60.35 ± 0.26	74.20 ± 0.13
$(3,4,3)$	81.80 ± 0.28	79.10 ± 0.35	72.41 ± 0.36	83.71 ± 0.68
$(4,4)$	92.50 ± 0.29	92.81 ± 0.16	92.19 ± 0.39	89.85 ± 0.51
$(4,3)$	93.08 ± 0.40	92.72 ± 0.69	91.45 ± 0.67	91.28 ± 0.32
$(3,3)$	95.39 ± 0.38	$\mathbf{93.62 \pm 0.06}$	$\mathbf{94.82 \pm 0.36}$	$\mathbf{92.43 \pm 0.22}$
(3)	93.65 ± 0.34	93.28 ± 0.22	93.02 ± 0.17	92.37 ± 0.26
(2)	$\mathbf{95.64 \pm 0.32}$	93.29 ± 0.47	93.03 ± 0.45	92.04 ± 0.21

Best results are in bold

Experiments

Table 3 Purification performance of TendiffPure on MNIST evaluated by the pre-trained LeNet classifier

Model	Standard accuracy (%)	Robust accuracy (%)		
		Gaussian noise	Salt and pepper noise	AutoAttack
DDPM	98.97 ± 0.52	$\mathbf{98.93 \pm 0.05}$	98.03 ± 0.34	99.27 ± 0.22
DDIM	81.25 ± 0.30	62.18 ± 0.42	22.30 ± 0.25	83.17 ± 0.41
TendiffPure (ours)	$\mathbf{99.27 \pm 0.22}$	98.68 ± 0.29	$\mathbf{98.70 \pm 0.12}$	$\mathbf{99.48 \pm 0.08}$

Best results are in bold

Table 6 Ablation studies of TendiffPure on MNIST evaluated by the pre-trained LeNet classifier

Rank	Standard accuracy (%)	Robust accuracy (%)		
		Gaussian noise	Salt and pepper noise	AutoAttack
$(3, 3, 3)$	90.77 ± 0.22	68.51 ± 0.08	63.51 ± 0.38	91.67 ± 0.14
$(4, 4, 4)$	92.83 ± 0.30	74.75 ± 0.22	71.16 ± 0.27	91.93 ± 0.35
$(3, 4, 3)$	94.41 ± 0.14	79.16 ± 0.48	79.21 ± 0.20	94.17 ± 0.44
$(4, 4)$	97.36 ± 0.43	91.57 ± 0.30	90.61 ± 0.43	97.28 ± 0.29
$(3, 3)$	97.74 ± 0.28	95.05 ± 0.12	93.75 ± 0.39	97.12 ± 0.26
$(4, 3)$	$\mathbf{99.27 \pm 0.22}$	$\mathbf{98.68 \pm 0.29}$	$\mathbf{98.70 \pm 0.12}$	$\mathbf{99.48 \pm 0.08}$
$(2, 3)$	98.94 ± 0.24	$\mathbf{98.68 \pm 0.15}$	98.08 ± 0.30	98.78 ± 0.41
(2)	98.24 ± 0.27	98.34 ± 0.20	97.38 ± 0.30	98.86 ± 0.41

Best results are in bold

Conclusions

1. We proposed TendiffPure as a compressed diffusion model for purification without compromise to performance.

2. We explored the impact of tensor-train decomposition to the performance of TendiffPure.

3. In the future work, we aim to theoretically analyze the effect of tensor decomposition methods on diffusion models for purification.

Mingyuan BAI is currently a postdoctoral researcher with Tensor Learning Team at RIKEN Center of Advanced Intelligence Project. She received her BCom (Honours Division I) and PhD degrees from The University of Sydney, NSW, Australia, in 2018 and 2022, respectively. Her research interests include generative models, adversarial robustness, and deep learning.

Derun ZHOU received his BS degree in School of Mathematics in 2022 from Soochow University, Soochow, Jiangsu Province, China. He is currently pursuing his MS degree in Computing Science at Tokyo Institute of Technology. His research interests focus on information geometry and tensor decomposition.

Qibin ZHAO is currently the team leader of Tensor Learning Team at RIKEN Center of Advanced Intelligence Project. He received his PhD degree from Shanghai Jiao Tong University, Shanghai, China, in 2009. He was a Research Scientist with the Brain Science Institute, RIKEN, Tokyo, Japan, from 2009 to 2017. He has published more than 150 scientific articles and coauthored two monographs on tensor networks. His research interests include machine learning, tensor factorization and tensor networks, and brain signal processing. He serves as the Area Chair for ML conferences of Conference on Neural Information Processing Systems (NeurIPS), International Conference on Machine Learning (ICML), and Asian Conference on Machine Learning (ACML), and an Action Editor for Neural Networks and Transactions on Machine Learning Research.