Figure 7: The distribution of the FPR of the BlindMI-Diff-w/ [24].

Figure 8: The evaluation of the existing MI attacks (e.g., *the attacker-side precision, recall, f1-score and FPR*).
.

Figure 9: The effect of differential distance between two datasets on the Membership Advantage.

Figure 10: The effect of the ratio of the samples that are made no inferences by an MI attack.

(a) CIFAR100 (b) CIFAR10 (c) CH_MNIST (d) ImageNet (e) Purchase100

Figure 11: The comparisons of the effect of the distance between data samples of the target dataset (DisBD) and the differential difference between two datasets (DiffDis) on MA.
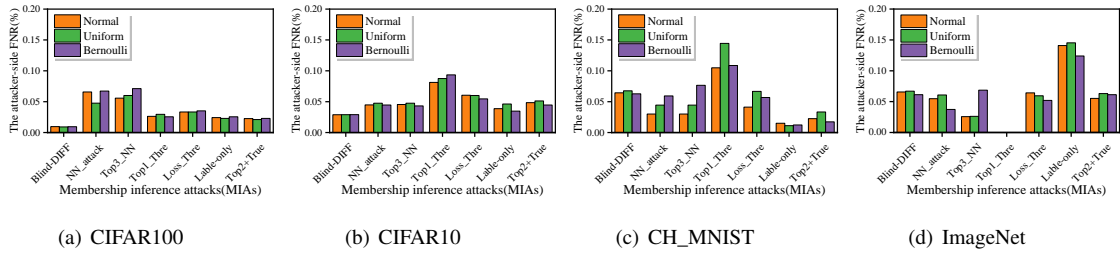

(a) CIFAR100 (b) CIFAR10 (c) CH_MNIST (d) ImageNet

Figure 12: The attacker-side FNR of the distance distribution of the target datasets obeying normal, uniform and bernoulli distributions.
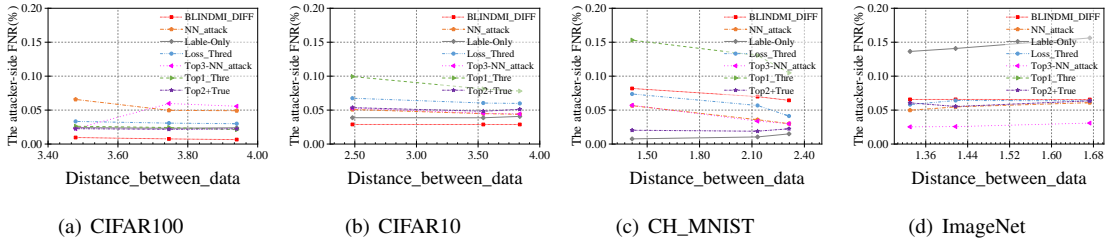

(a) CIFAR100 (b) CIFAR10 (c) CH_MNIST (d) ImageNet

Figure 13: The effect of the distance between data samples in the target dataset on the attacker-side FNR.

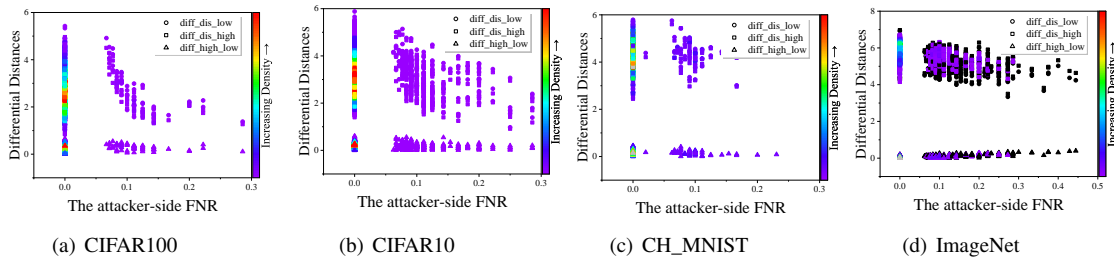(a) CIFAR100 (b) CIFAR10 (c) CH_MNIST (d) ImageNet

Figure 14: The effect of the differential distance between two datasets on attacker-side FNR.

Table 10: The average distance between data samples (DisBD) and the differential distance between two datasets (DiffDis) change on the MA (C_MA).

Dataset	C_MA	average DisBD	average DiffDis
CIFAR100	10%	0.143	**0.107**
	20%	0.230	**0.099**
	30%	0.349	**0.138**
	40%	0.460	**0.143**
	50%	0.630	**0.257**
CIFAR10	10%	0.113	**0.082**
	20%	0.179	**0.115**
	30%	0.299	**0.182**
	40%	0.440	**0.238**
	50%	0.544	**0.320**
	60%	0.659	**0.389**
	70%	0.793	**0.545**
CH_MNIST	10%	0.140	**0.091**
	20%	0.249	**0.158**
	30%	0.335	**0.237**
	40%	0.476	**0.328**
	50%	0.638	**0.408**
	60%	0.843	**0.547**
ImageNet	10%	0.268	**0.225**
	20%	0.580	**0.288**
	30%	0.805	**0.379**