APPENDIX

A. Common Privacy Compression Scenario

Consider a typical PC scenario: Yang wants to use an image recognition service on a autonomous AI server provided by Wang on cloud while being cautious of potential privacy threats from malicious attackers. Yang minimizes exposure risks before sending the images to the cloud by applying a privacy compression mechanism to his healthcare images. Wang then processes the privatized images for his service. The central challenge of a PC system lies in balancing utility (the informational value of the utility service provider) and privacy (the information obtained by adversaries), which can be effectively analyzed using the information bottleneck theory. This analysis has led to the development of Differential Mutual Information (DMI) [1], [2], providing quantitative guidance for designing these mechanisms.

B. Define the Network Structure

"Conv1" refers to a single Conv block; "Conv2" indicates two Conv blocks; and "Conv3" represents three Conv blocks. Similarly, just like "Conv1," "ConvRes1" denotes a single ConvRes1 block. The same naming pattern applies to "DeConv" and "DeConvRes" blocks.

1) Conv block: The Conv block is shown in Figure 1. The output unit for Conv1 is 6. The output unit for Conv2 is 16.

```
Model: "conv_block"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             multiple                  1216

 max_pooling2d (MaxPooling2D  multiple                 0
 )

=================================================================
```

Fig. 1. Conv block

2) ConvRes block: The ConvRes block is shown in Figure 2. The output unit for ConvRes1 is 6. The output unit for ConvRes2 is 16.

```
Model: "conv_res_block"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d (Conv2D)             multiple                  228

 batch_normalization (BatchN  multiple                 12
 ormalization)

 conv2d_1 (Conv2D)           multiple                  228

 batch_normalization_1 (Batc  multiple                 12
 hNormalization)

 max_pooling2d (MaxPooling2D  multiple                 0
 )

=================================================================
```

Fig. 2. ConvRes block

3) DeConv block: The DeConv block is shown in Figure 3. The output unit for DeConvRes is 32 or 3.

4) DeConvRes block: The DeConvRes block is shown in Figure 4. The output unit for DeConvRes is 32 or 3.

```
Model: "de_conv_block"
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d_transpose (Conv2DTra  multiple                 448
 nspose)

=================================================================
```

Fig. 3. DeConv block

```
_________________________________________________________________
 Layer (type)                Output Shape              Param #
=================================================================
 conv2d_transpose (Conv2DTra  multiple                 168
 nspose)

 batch_normalization (BatchN  multiple                 24
 ormalization)

 conv2d_transpose_1 (Conv2DT  multiple                 330
 ranspose)

 batch_normalization_1 (Batc  multiple                 24
 hNormalization)

 conv2d_transpose_2 (Conv2DT  multiple                 24
 ranspose)

=================================================================
Total params: 570
Trainable params: 546
Non-trainable params: 24
```

Fig. 4. DeConvRes block

C. Final Parameters

Just list final parameters for each dataset.

1) Final Parameters: Face Recognition: The final parameters for face recogniton are shown in Table I.

TABLE I
PARAMETERS FOR FACE RECOGNITION

Symbol	AutoAgent1	AutoAgent2
PA_{DcNN}	DeConvRes3	DeConvRes3
η_{DcNN}	$3 * 10^{-3}$	$2 * 10^{-3}$
$\beta_{1,DcNN}$	0.9	0.8919
$\beta_{2,DcNN}$	0.9981	0.9993
ρ_{RR}	0.002	0.001
ρ_{NKR}	0.9952	0.9976
MD	2564	2058
Ker	RBF	RBF
σ_K	0.002	0.002
σ_P	1	4
PA_U	ResNet50V2	ResNet50V2
η_U	$9 * 10^{-4}$	10^{-3}
$\beta_{1,U}$	0.9	0.8846
$\beta_{2,U}$	0.9973	0.9987
PA_{pc}	Conv2	Conv2
η_{pc}	10^{-3}	$2 * 10^{-3}$
$\beta_{1,pc}$	0.8394	0.895
$\beta_{2,pc}$	0.9959	0.9981
e	170	137
n	1	1

2) Final Parameters: Chest X-ray Recognition: The final parameters for X-ray recogniton are shown in Table II.

TABLE II
PARAMETERS FOR X-RAY RECOGNITION

Symbol	AutoAgent1	AutoAgent2
PA_{DcNN}	DeConv2	DeConv2
η_{DcNN}	$5 * 10^{-4}$	$5 * 10^{-4}$
$\beta_{1,DcNN}$	0.8780	0.8566
$\beta_{2,DcNN}$	0.9981	0.9904
ρ_{RR}	0.003	0.001
ρ_{NKR}	0.0021	0.0007
MD	4312	4999
Ker	RBF	RBF
σ_K	0.003	0.003
σ_P	5	3
PA_U	ResNet50V2	ResNet50V2
η_U	$9 * 10^{-4}$	10^{-3}
$\beta_{1,U}$	0.8163	0.8747
$\beta_{2,U}$	0.9876	0.9895
PA_{pc}	Conv2	Conv2
η_{pc}	$2 * 10^{-3}$	$8 * 10^{-4}$
$\beta_{1,pc}$	0.8531	0.8164
$\beta_{2,pc}$	0.9907	0.9680
e	113	86
n	2	1

3) Final Parameters: HAR Recognition: The final parameters for face recogniton are shown in Table III.

TABLE III
PARAMETERS FOR HAR RECOGNITION

Symbol	AutoAgent1	AutoAgent2
PA_{DcNN}	DeConv4	DeConv4
η_{DcNN}	$9 * 10^{-4}$	10^{-3}
$\beta_{1,DcNN}$	0.8763	0.8967
$\beta_{2,DcNN}$	0.9991	0.9982
ρ_{RR}	0.004	0.001
ρ_{NKR}	0.0859	0.0979
MD	4013	4996
Ker	Polynomial	RBF
σ_K	0.006	0.001
σ_P	2	2
PA_U	ResNet50V2	CapsNet
η_U	$6 * 10^{-4}$	$8 * 10^{-4}$
$\beta_{1,U}$	0.8273	0.8458
$\beta_{2,U}$	0.9996	0.9993
PA_{pc}	Conv2	Conv2
η_{pc}	$9 * 10^{-4}$	$2 * 10^{-3}$
$\beta_{1,pc}$	0.8972	0.8899
$\beta_{2,pc}$	0.9781	0.9541
e	167	169
n	32	32

REFERENCES

[1] S.-Y. Kung, “Compressive privacy: From information\/estimation theory to machine learning [lecture notes],” *IEEE Signal Processing Magazine*, vol. 34, no. 1, pp. 94–112, 2017.

[2] S. Kung, “A compressive privacy approach to generalized information bottleneck and privacy funnel problems,” *Journal of the Franklin Institute*, vol. 355, no. 4, pp. 1846–1872, 2018, special Issue on Recent advances in machine learning for signal analysis and processing. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0016003217303162