

Supplementary Materials: Once-for-all: Efficient Visual Face Privacy Protection via Person-specific Veils

Anonymous Authors

A PROOF

Here, we provide a proof that U remains constant. In our definition, the $CH(F(X^P))$ is spanned by a set of orthonormal basis vectors that can be calculated by $F(x_i^P)$ ($i = 1, 2, 3, \dots, n_p$). Let us denote it as $(\beta_1, \beta_2, \dots, \beta_m, m \leq n_p)$. Therefore, each $F(x_i^P)$ can be represented as

$$F(x_i^P) = k_i^1 \beta_1 + k_i^2 \beta_2 + \dots + k_i^m \beta_m, \quad (1)$$

where $k_i^1, k_i^2, \dots, k_i^m$ is the coefficient of corresponding linear representation. Then, the definition of $CH(F(X^P))$ can be transformed as

$$\begin{aligned} CH(F(X^P)) &= \sum_{i=1}^{n_p} \sum_{j=1}^{m_p} w_i^p k_i^j \beta_j, \\ \text{s.t. } w_i^p &\geq 0, \sum_{x_i^P \in X^P} w_i^p = 1. \end{aligned} \quad (2)$$

Since w_i^p is a constant, we can extract them from the equation. Thus, we can substitute $W^p = (w_1^p, w_2^p, \dots, w_{n_p}^p)^T$ into the equation and obtain

$$\begin{aligned} CH(F(X^P)) &= \sum_{i=1}^{n_p} \sum_{j=1}^{m_p} k_i^j \beta_j W^p, \\ \text{s.t. } W^p &\geq 0, \mathbf{1}^T W^p = 1. \end{aligned} \quad (3)$$

Therefore, by using SVD to $CH(F(X^P))$, we can get the U that is composed of the orthogonal basis vectors. Once get the $F(x_i^P)$, orthogonal basis vectors remain constant and thus U also remains constant. Eventually, the generation of person-specific veils can be regarded as a problem in solving W^p .

B MORE ROBUSTNESS ANALYSIS

Apart from Gaussian noise, we also assess the impact of salt-and-pepper noise and median filtering on the visual privacy protection performance of our scheme. The experimental results are presented in Fig. 1 and Fig. 2. It can be found that when the *Salt_rate* surpasses 0.04, the MSR of the protected images starts to decrease. In addition, despite the small *kernel_size* of median filtering, the MSR diminishes sharply. Compared to the addition of noise, the removal of noise has a more pronounced impact on identity preservation. We infer that the filtering process alters the values of neighboring pixels, which has a greater impact on the identity feature vectors.

C MORE PERFORMANCE ON VISUAL FACE PRIVACY PROTECTION

Firstly, we additionally present some protected images on the Privacy-Celebrities dataset when the testing images are different from the training images, which is shown in Fig. 3. Secondly, we also evaluate the performance of our scheme on Privacy-Commons datasets.

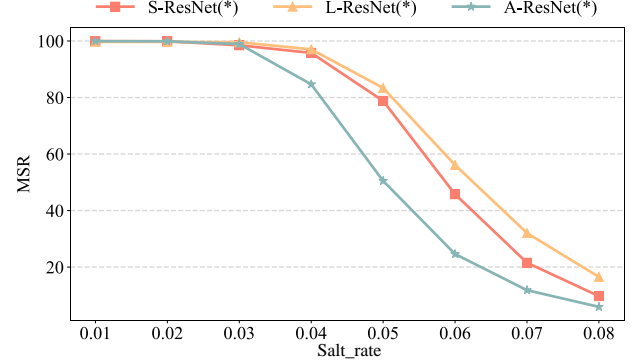


Figure 1: Robustness testing of protected images against salt and pepper noise. 'Salt_rate' means the proportion of white pixels added to the image and '*' implies that the testing model is identical to the surrogate model.

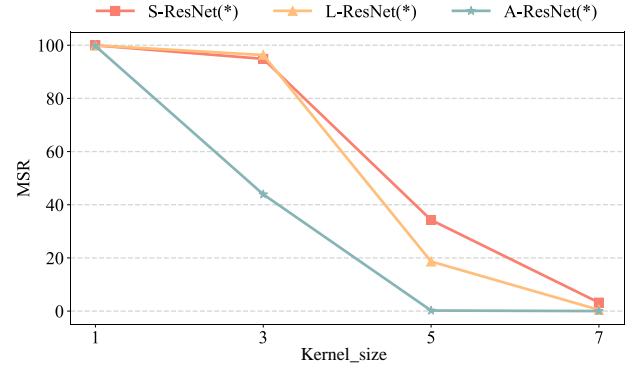


Figure 2: Robustness testing of protected images against median filtering. 'Kernel_size' denotes the kernel size of the window size for computing the median value.

Meanwhile, the qualitative results are illustrated in Fig. 4, and the quantitative results are shown in Fig. 5. Thirdly, we assess the performance of our scheme in supporting recoverability on the Privacy-Commons dataset in Table 1.

Table 1: The SSIM values and LPIPS values of recovered images on the Privacy-Commons dataset.

Method	Source Model	SSIM(↑)	LPIPS(↓)
ours	S-ResNet	0.868	0.046
	L-ResNet	0.869	0.047
	A-ResNet	0.869	0.046

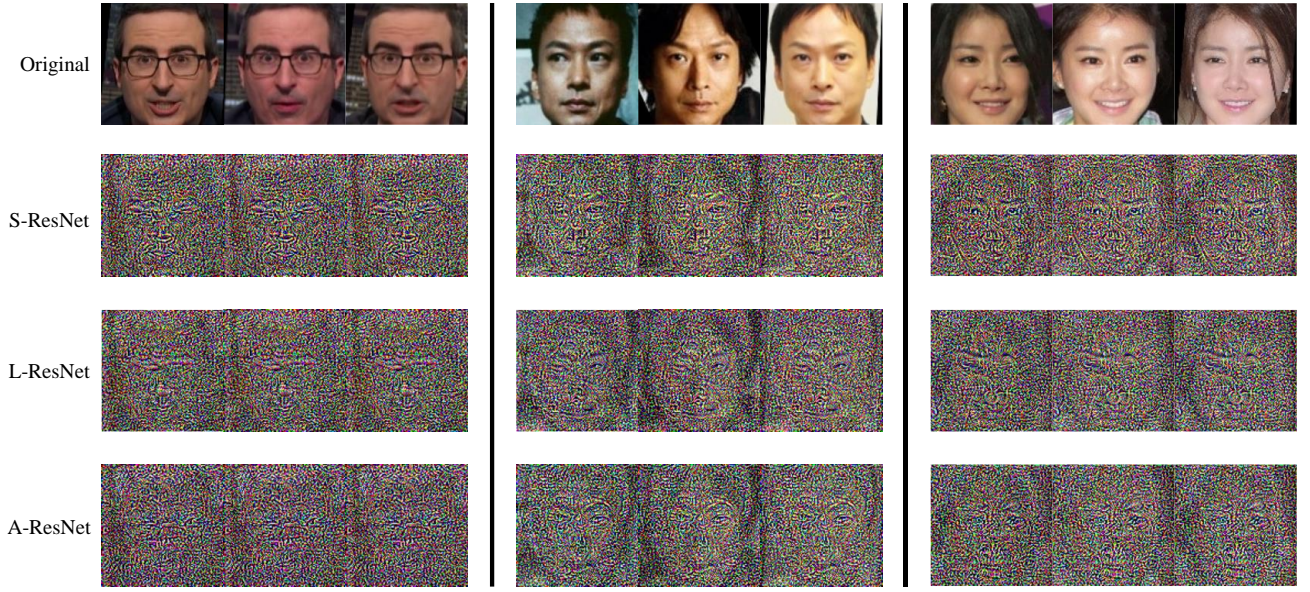


Figure 3: Some protected images on the Privacy-Celebrities dataset. Note that the testing images are distinct from the training images.

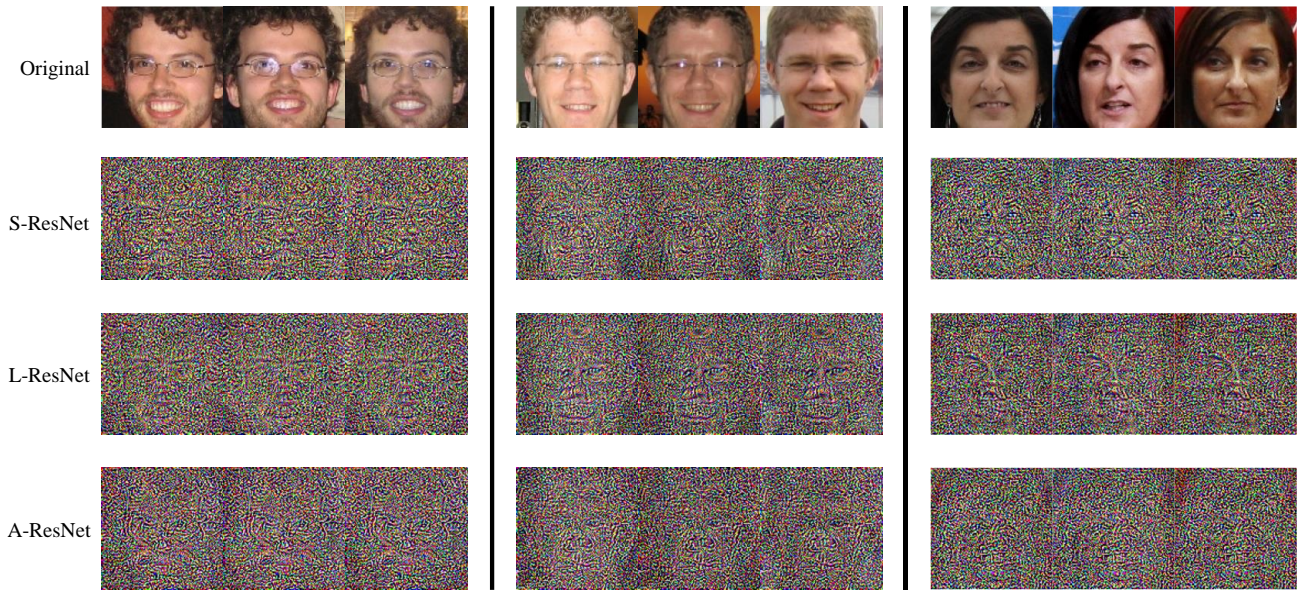


Figure 4: Some protected images on the Privacy-Commons dataset. Each image within every subplot shares the same identity.

D MORE DISCUSSION

Application Scenarios. Visual privacy protection is becoming increasingly essential in software applications and is being promoted by various sectors and institutions. These entities are encouraging service providers to proactively offer protective functionalities to users. It ensures that the process of privacy interaction is regulated and protected by the law, which allows a broader range of service recipients to benefit from it. Considering the limited computational resources available to ordinary users, it is preferable

for service providers to perform the entire training process of veil generation and provide corresponding service interfaces. It enables the users to receive the necessary assistance without the burden of resource-intensive tasks. By adopting our scheme, which effectively addresses the need for assistance in visual privacy protection, service providers can empower users with efficient means of protecting their visual privacy in real-time scenarios.

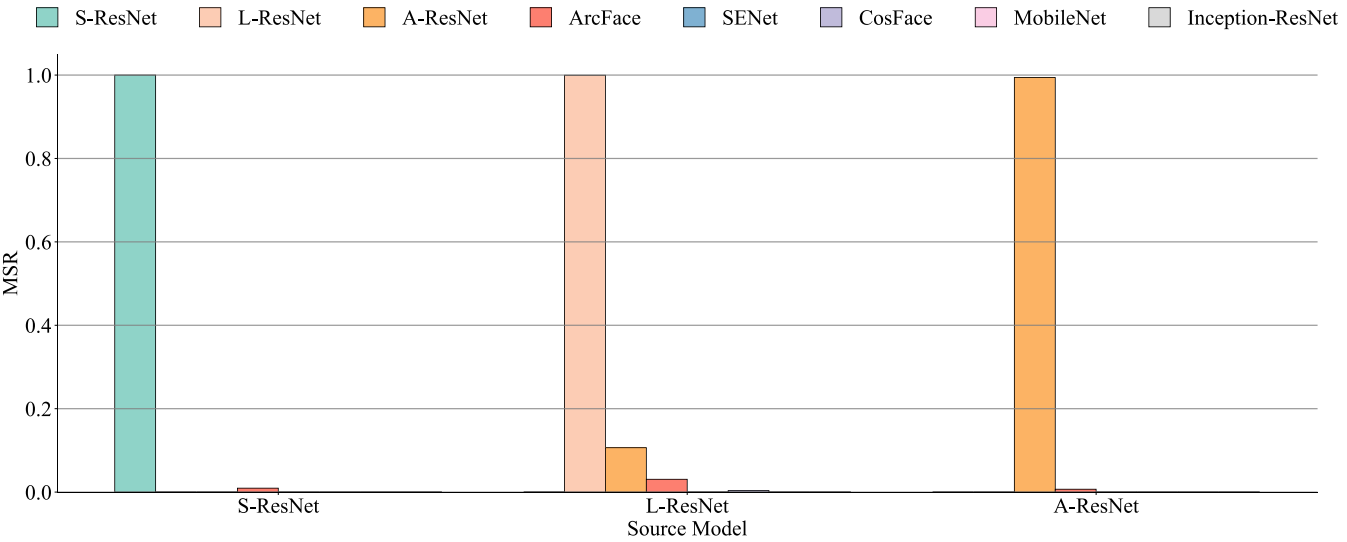


Figure 5: The MSR of the protected images tested across different models on the Privacy-Commons dataset.