**NinjaDesc: Content-Concealing Visual Descriptors via Adversarial Learning**

Tony Ng\(^1,2\)  Hyo Jin Kim\(^1\)†  Vincent Lee\(^1\)  Daniel Detone\(^1\)  Tsun-Yi Yang\(^1\)
Tianwei Shen\(^1\)  Eddy Ilg\(^1\)  Vassileios Balntas\(^1\)  Krystian Mikolajczyk\(^2\)  Chris Sweeney\(^1\)

\(^1\)Reality Labs, Meta  \(^2\)Imperial College London

**Abstract**

In the light of recent analyses on privacy-concerning scene revelation from visual descriptors, we develop descriptors that conceal the input image content. In particular, we propose an adversarial learning framework for training visual descriptors that prevent image reconstruction, while maintaining the matching accuracy. We let a feature encoding network and image reconstruction network compete with each other, such that the feature encoder tries to impede the image reconstruction with its generated descriptors, while the reconstructor tries to recover the input image from the descriptors. The experimental results demonstrate that the visual descriptors obtained with our method significantly deteriorate the image reconstruction quality with minimal impact on correspondence matching and camera localization performance.

1. **Introduction**

Local visual descriptors are fundamental to a wide range of computer vision applications such as SLAM [13, 36, 38, 41], SFM [1, 59, 66], wide-baseline stereo [27, 39], camera calibration [44], tracking [22, 40, 46], image retrieval [3, 4, 42, 61, 71, 72], and camera pose estimation [11, 15, 48, 50, 55, 56, 69, 70]. These descriptors represent local regions of images and are used to establish local correspondences between and across images and 3D models.

The descriptors take the form of vectors in high-dimensional space, and thus are not directly interpretable by humans. However, researchers have shown that it is possible to reveal the input images from local visual descriptors [8, 14, 74]. With the recent advances in deep learning, the quality of the reconstructed image content has been significantly improved [9, 47]. This pose potential privacy concerns for visual descriptors if they are used for sensitive data without proper encryption [9, 64, 74].

To prevent the reconstruction of the image content from visual descriptors, several methods have been proposed. These methods include obfuscating keypoint locations by lifting them to lines that pass through the original points [19, 60, 64, 65], or to affine subspaces with augmented adversarial feature samples [16] to increase the difficulty of recovering the original images. However, recent work [7] has demonstrated that the closest points between lines can yield a good approximation to the original points locations, allowing descriptor inversion.

In this work, we explore whether such local feature inversion could be mitigated at the descriptor level. Ideally, we want a descriptor that does not reveal the image content without a compromise in its performance. This may seem counter-intuitive due to the trade-off between utility and privacy discussed in the recent analysis on visual descriptors [9], where the utility is defined as matching accuracy, and the privacy is defined as non-invertibility of the descriptors. The analysis showed that the more useful the descriptors are for correspondence matching, the easier it is...
to invert them. To minimize this trade-off, we propose an adversarial approach to train visual descriptors.

Specifically, we optimize our descriptor encoding network with an adversarial loss for descriptor invertibility, in addition to the traditional metric learning loss for feature correspondence matching. For the adversarial loss, we jointly train an image reconstruction network to compete with the feature descriptor network in revealing the original image content from the descriptors. In this way, the feature descriptor network learns to hinder the image reconstruction network by generating visual descriptors that conceal the original image content, while being optimized for correspondence matching.

In particular, we introduce an auxiliary encoder network \textit{NinjaNet} that can be trained with any existing visual descriptors and transform them to our content-concealing \textit{NinjaDesc}, as illustrated in Fig. 1. In the experiments, we show that visual descriptors trained with our adversarial learning framework lead to only marginal drop in performance for feature matching and visual localization tasks, while significantly reducing the visual similarity of the reconstruction to the original input image.

One of the main benefits of our method is that we can control the trade-off between utility and privacy by changing a single parameter in the loss function. In addition, our method generalizes to different types of visual descriptors, and different image reconstruction network architectures.

In summary, our main innovations are as follows: \textbf{a)} We propose a novel adversarial learning framework for visual descriptors to prevent reconstructing original input image content from the descriptors. We experimentally validate that the obtained descriptors significantly deteriorate the image quality from descriptor inversion with only marginal drop in matching accuracy using standard benchmarks for matching (HPatches [5]) and visual localization (Aachen Day-Night [57,77]). \textbf{b)} We empirically demonstrate that we can effectively control the trade-off between utility (matching accuracy) and privacy (non-invertibility) by changing a single training parameter. \textbf{c)} We provide ablation studies by using different types of visual descriptors, image reconstruction network architectures and scene categories to demonstrate the generalizability of our method.

2. Related work

This section discusses prior work on visual descriptor inversion and the state-of-the-art descriptor designs that attempt to prevent such inversion.

\textbf{Inversion of visual descriptors.} Early results of reconstructing images from local descriptors was shown by Weinzaepfel \textit{et al.} [74] by stitching the image patches from a known database with the closest distance to the input SIFT [33] descriptors in the feature space. d’Angelo \textit{et al.} [8] used a deconvolution approach on local binary descriptors such as BRIEF [6] and FREAK [2]. Vondrick \textit{et al.} [73] used paired dictionary learning to invert HoG [78] features to reveal its limitations for object detection. On the global descriptor side, Kato and Harada [28] demonstrated image reconstruction from bag-of-words (BoW) descriptors [63]. However, the quality of reconstructions by these early works were not sufficient to raise concerns about privacy or security.

Subsequent work introduced methods that steadily improved the quality of the reconstructions. Mahendran and Vedaldi [35] used a back-propagation technique with a natural image prior to invert CNN features as well as SIFT [32] and HOG [78]. Dosovitskiy and Brox [14] trained up-convolutional networks that estimate the input image from features in a regression fashion, and demonstrated superior results on both classical [33, 43, 78] and CNN [30] features. In the recent work, descriptor inversion methods have started to leverage larger and more advanced CNN models as well as employ advanced optimization techniques. Pitálgua \textit{et al.} [47] and Dangwal \textit{et al.} [9] demonstrated sufficiently high reconstruction qualities, revealing not only semantic information but also details in the original images.

\textbf{Preventing descriptor inversion for privacy.} Descriptive inversion techniques may raise privacy concerns [9, 47, 64, 74]. For example, in computer vision systems where the visual descriptors are transferred between the device and the server, an honest-but-curious server may try to exploit the descriptors sent by the client device. In particular, many large-scale camera localization systems adopt cloud computing and storage, due to limited processing power, memory, and storage on mobile devices. Cryptographic methods like homomorphic encryption [17, 54, 76] can be used to protect descriptors, but they are too computationally expensive for large-scale applications.

Proposed by Speciale \textit{et al.} [64], the line-cloud representation obfuscate 2D/3D point locations in the map building process [18, 19, 60] without compromising the accuracy in localization. However, since the descriptors are unchanged, Chelani \textit{et al.} [7] showed that line-clouds are vulnerable to inversion attacks if the underlying point-cloud is recovered.

Recently, Dusmanu \textit{et al.} [16] proposed a privacy-preserving visual descriptor via lifting descriptors to affine subspaces, which conceals the visual content from inversion attacks. However, this comes with a significant cost on the descriptor’s utility in downstream tasks. Our work differs from [16] in that we propose a learned content-concealing descriptor and explicitly train it for utility retention to achieve a better trade-off between the two.

3. Method

We propose an adversarial learning framework for obtaining content-concealing visual descriptors, by introduc-
learning loss from \( [68] \) to optimize NinjaDesc (\( d \))

allowing for easy implementation of triplet-loss training.

subsets of patches labelled as positive and negative pairs,

loss. We use the UBC dataset \([20]\) which contains three

descriptor training approach \([37, 67, 68]\). The

for correspondence matching and visual localization \([27]\).

since it is one of the top-performing descriptors

many of our experiments, we adopt SOSNet \([68]\) as our base

but prevents from high-quality reconstruction of images. In

contains the matching performance of the original descriptor,

local descriptors. The encoded NinjaDesc descriptor main-

to make it flexible in accepting different types of existing

transforms it into a content-concealing NinjaDesc,

3.1. NinjaNet: the content-concealing encoder

In order to conceal the visual content of a local descriptor

while maintaining its utility, we need a trainable encoder

which transforms the original descriptor space to a different

one, where visual information essential for reconstruction is

reduced. Our NinjaNet encoder \( \Theta \) is implemented by an

MLP shown in Fig. 2. It takes a base descriptor \( d_{\text{base}} \), and transforms it into a content-concealing NinjaDesc, \( d_{\text{ninja}} \):

where

\[
d_{\text{ninja}} = \Theta(d_{\text{base}})
\]

The design of NinjaNet is light-weight and plug-and-play,
to make it flexible in accepting different types of existing

local descriptors. The encoded NinjaDesc descriptor maintains the matching performance of the original descriptor, but prevents from high-quality reconstruction of images. In many of our experiments, we adopt SOSNet \([68]\) as our base descriptor since it is one of the top-performing descriptors for correspondence matching and visual localization \([27]\).

Utility initialization. To maintain the utility (i.e. accuracy for downstream tasks) of our encoded descriptor, we use a patch-based descriptor training approach \([37, 67, 68]\). The initialization step trains NinjaNet via a triplet-based ranking loss. We use the UBC dataset \([20]\) which contains three subsets of patches labelled as positive and negative pairs, allowing for easy implementation of triplet-loss training.

Utility loss. We extract the base descriptors \( d_{\text{base}} \) from image patches \( x_{\text{patch}} \) and train NinjaNet (\( \Theta \)) with the descriptor learning loss from \([68]\) to optimize NinjaDesc (\( d_{\text{ninja}} \)).

\[
\mathcal{L}_{\text{util}}(x_{\text{patch}}; \Theta) = \mathcal{L}_{\text{triplet}}(d_{\text{ninja}}) + \mathcal{L}_{\text{reg}}(d_{\text{ninja}}),
\]

where \( \mathcal{L}_{\text{reg}}(\cdot) \) is the second-order similarity regularization term \([68]\). We always freeze the weights of the base descriptor network, including the joint training process in Sec. 3.3.

3.2. Descriptor inversion model

For our proposed adversarial learning framework, we utilize a descriptor inversion network as the adversary to reconstruct the input images from our NinjaDesc. We adopt the UNet-based \([52]\) inversion network from prior work \([9, 47]\). Following Dangwal et al. \([9]\), the inversion model \( \Phi \) takes as input the sparse feature map \( F_{\Theta} \in \mathbb{R}^{H \times W \times C} \) composed from the descriptors and their keypoints, and predicts the RGB image \( \hat{I} \in \mathbb{R}^{h \times w \times 3} \), i.e.

\[
\hat{I} = \Phi(F_{\Theta}).
\]

We denote \( (H, W), (h, w) \) as the resolutions of the sparse feature image and the reconstructed RGB image, respectively. \( C \) is the dimensionality of the descriptor. The detailed architecture is provided in the supplementary.

Reconstruction loss. The descriptor inversion model \( \Phi \) is optimized under a reconstruction loss which is composed of two parts. The first loss is the mean absolute error (MAE) between the predicted \( \hat{I} \) and input \( I \) images,

\[
\mathcal{L}_{\text{mae}} = \sum_{i} \sum_{j} |I_{i,j} - \hat{I}_{i,j}|_1.
\]

The second loss is the perceptual loss, which is the L2 distance between intermediate features of a VGG16 \([62]\) network pretrained on ImageNet \([10]\).

\[
\mathcal{L}_{\text{perc}} = \frac{3}{2} \sum_{k=1}^{3} \sum_{i} \sum_{j} \|\psi_{VGG}^{k,i,j}(I) - \psi_{VGG}^{k,i,j}(\hat{I})\|_2^2,
\]

where \( \psi_{VGG}^{k,i,j}(I) \) are the feature maps extracted at layers \( k \in \{2, 9, 16\} \), and \( (h_k, w_k) \) is the corresponding resolution.

The reconstruction loss is the sum of the two terms

\[
\mathcal{L}_{\text{recon}}(x_{\text{image}}; \Phi) = \mathcal{L}_{\text{mae}} + \mathcal{L}_{\text{perc}}.
\]

where \( x_{\text{image}} \) denote the image data term that includes both the descriptor feature map \( F_{\Theta} \) and the RGB image \( I \).

Reconstruction initialization. For the joint adversarial training described in Sec. 3.3, we initialize the the inversion model using the initialized NinjaDesc in Sec. 3.1. This part is done using the MegaDepth \([31]\) dataset, which contains images of landmarks across the world. For the keypoint detection we use the Harris corners \([23]\) in our experiments.

3.3. Joint adversarial training

The central component of engineering our content-concealing NinjaDesc is the joint adversarial training step, which is illustrated in Fig. 3 and elaborated as pseudo-code in Algorithm 1. We aim to minimize trade-off between utility and privacy, which are the two competing objectives. Inspired by methods using adversarial learning \([21, 53, 75]\), we formulate the optimization of utility and privacy trade-off as an adversarial learning process. The objective of the
A. Utility (Matchability)

![Diagram of utility matchability](image)

1. $\mathcal{L}_{\text{util}} = \mathcal{L}_{\text{triplet}} + \mathcal{L}_{\text{reg}}$

B. Reconstruction

![Diagram of reconstruction](image)

Joint Adversarial Training

1. $\mathcal{L}_{\text{util}} - \lambda \mathcal{L}_{\text{recon}}$

2. $\mathcal{L}_{\text{recon}}$

Algorithm 1: Pseudo-code for the joint adversarial training process of NinjaDesc

1: NinjaNet: $\Theta_0 \leftarrow $ initialize with Eqn. 2
2: Desc. inversion model: $\Phi_0 \leftarrow $ initialize with Eqn. 5
3: $\lambda \leftarrow $ set privacy parameter
4: for $i \leftarrow 1$, number of iterations do
5:   if $i = 0$ then
6:     $\Theta \leftarrow \Theta_0$, $\Phi \leftarrow \Phi_0$
7:   end if
8:   Compute $\mathcal{L}_{\text{util}}$ from $x_{\text{patch}}$ and $\Theta$.
9:   Extract sparse features on $x_{\text{image}}$ with $\Theta$, reconstruct image with $\Phi$
10:  and compute $\mathcal{L}_{\text{recon}} (x_{\text{image}}; \Theta, \Phi)$.
11:  Update weights of $\Theta$:
12:     $\Theta \leftarrow \nabla_{\Theta} \left( \mathcal{L}_{\text{util}} - \lambda \mathcal{L}_{\text{recon}} \right)$.
13:  Extract sparse features on $x_{\text{image}}$ with $\Theta'$, reconstruct image with $\Phi'$
14:  Update weights of $\Phi'$:
15:     $\Phi \leftarrow \nabla_{\Phi} \mathcal{L}_{\text{util}}$.
16: end for

This brings us to the two separate optimization objectives for $\Theta$ and $\Phi$ that we will describe in the following. For the inversion model $\Phi$, the objective remains the same as in Eqn. 6:

$$\mathcal{L}_{\Phi} = \mathcal{L}_{\text{recon}} (x_{\text{image}}; \Theta, \Phi).$$  

However, for maintaining utility, NinjaNet with weights $\Theta$ is also optimized with the utility loss $\mathcal{L}_{\text{util}} (x_{\text{patch}}; \Theta)$ from Eqn. 2. In conjunction with the maximization by $\Theta$ from Eqn. 6, the loss for NinjaNet becomes

$$\mathcal{L}_{\Theta} = \mathcal{L}_{\text{util}} (x_{\text{patch}}; \Theta) - \lambda \mathcal{L}_{\text{recon}} (x_{\text{image}}; \Theta, \Phi),$$  

where $\lambda$ controls the balance of how much $\Theta$ prioritizes content concealment over utility retention, i.e. the privacy parameter. In practice, we optimize $\Theta$ and $\Phi$ in an alternating manner, such that $\Theta$ is not optimized in Eqn. 8 and $\Phi$ is not optimized in Eqn. 9. The overall objective is then

$$\Theta^*, \Phi^* = \arg\min_{\Theta, \Phi} (\mathcal{L}_{\Theta} + \mathcal{L}_{\Phi}).$$

3.4. Implementation details

The code is implemented using PyTorch [45]. We use Kornia [51]'s implementation of SIFT for GPU acceleration. For all training, we use the Adam [29] optimizer with $(\beta_1, \beta_2) = (0.9, 0.999)$ and $\lambda = 0$.

Utility initialization. We use the liberty set of the UBC patches [20] to train NinjaNet for 200 epochs and select the model with the lowest average FPR@95 in the other two sets (notredame and yosemite). The number of submodules in NinjaNet ($N$ in Fig. 2) is $N = 1$, since we observed no improvement in FPR@95 by increasing $N$. Dropout rate is 0.1. We use a batch-size of 1024 and learning rate of 0.01.

Reconstruction initialization. We randomly split MegaDepth [31] into train/validation/test split of ratio...
Figure 4. Qualitative results on landmark images. First column: original images overlaid with the 1000 (red) Harris corners [23]. Second column: reconstructions by the inversion model from raw SOSNet [68] descriptors extracted on those points. The last five columns show reconstruction from NinjaDesc with increasing privacy parameter $\lambda$. The SSIM and PSNR w.r.t. the original images are shown on top of each reconstruction. Best viewed digitally. Image credits: first 3 — Holidays dataset [26]; last — laylamoran4battersea (Flickr).

# 4. Experimental results

In this section, we evaluate NinjaDesc on the two criteria that guide its design — the ability to simultaneously achieve: (1) content concealment (privacy) and (2) utility (matching accuracy and camera localization performance).

## 4.1. Content concealment (Privacy)

We assess the content-concealing ability of NinjaDesc by measuring the reconstruction quality of descriptor inversion attacks. Here we assume the inversion model has access to the NinjaDesc and the input RGB images for training, i.e., $x_{image}$ in Sec. 3.2. We train the inversion model from scratch for NinjaDesc (Eqn. 5) on the train split of MegaDepth [31], and the best model with the highest SSIM on the validation set is selected for testing.

Recall in Eqn. 9, $\lambda$ is the privacy parameter controlling how much NinjaDesc prioritizes privacy over utility. The intuition is that, the higher $\lambda$ is, the more aggressive NinjaDesc tries to prevent reconstruction quality by the inversion model. We perform descriptor inversion on NinjaDesc that are trained with a range of $\lambda$ values to demonstrate its effect on reconstruction quality.

Fig. 4 shows qualitative results of descriptor inversion attacks when changing $\lambda$. We observe that $\lambda$ indeed fulfills the role of controlling how much NinjaDesc conceals the original image content. When $\lambda$ is small, e.g. 0.01, 0.1, the reconstruction is only slightly worse than that from the baseline SOSNet. As $\lambda$ increases to 0.25, there is a visi-

| RGB | SOSNet | $\lambda=0.01$ | $\lambda=0.1$ | $\lambda=0.25$ | $\lambda=1.0$ | $\lambda=2.5$ |
|-----|--------|----------------|----------------|----------------|----------------|----------------|
| ![Image](image1.png) | ![Image](image2.png) | ![Image](image3.png) | ![Image](image4.png) | ![Image](image5.png) | ![Image](image6.png) | ![Image](image7.png) |
| ![Image](image8.png) | ![Image](image9.png) | ![Image](image10.png) | ![Image](image11.png) | ![Image](image12.png) | ![Image](image13.png) | ![Image](image14.png) |
| ![Image](image15.png) | ![Image](image16.png) | ![Image](image17.png) | ![Image](image18.png) | ![Image](image19.png) | ![Image](image20.png) | ![Image](image21.png) |
| ![Image](image22.png) | ![Image](image23.png) | ![Image](image24.png) | ![Image](image25.png) | ![Image](image26.png) | ![Image](image27.png) | ![Image](image28.png) |
| ![Image](image29.png) | ![Image](image30.png) | ![Image](image31.png) | ![Image](image32.png) | ![Image](image33.png) | ![Image](image34.png) | ![Image](image35.png) |
| ![Image](image36.png) | ![Image](image37.png) | ![Image](image38.png) | ![Image](image39.png) | ![Image](image40.png) | ![Image](image41.png) | ![Image](image42.png) |
Figure 5. HPatches evaluation results. We compare the baseline SOSNet [68] vs. NinjaDesc, with 5 different levels of privacy parameter $\lambda$ (indicated by the number in parenthesis). All results are from models trained on the liberty subset of the UBC patches [20] dataset.

### Table 1. Quantitative results of the descriptor inversion on SOSNet vs. NinjaDesc, evaluated on the MegaDepth [31] test split. The arrows indicate higher/lower value is better for privacy.

| Metric          | SOSNet (Raw) | NinjaDesc ($\lambda$) |
|-----------------|--------------|------------------------|
| MAE (+)         | 0.104        | 0.001 0.01 0.1 0.25 1.0 2.5 |
| SSIM (-)        | 0.986        | 0.566 0.569 0.527 0.484 0.385 0.349 |
| PSNR (-)        | 17.904       | 18.037 16.826 17.821 17.671 13.367 12.010 |

Table 2. Visual localization results on Aachen-Day-Night v1.1 [77]. ‘Raw’ corresponds to the base descriptor in each column, followed by three $\lambda$ vales (0.1, 1.0, 2.5) for NinjaDesc.

| Query NNs Method | 0.25m, $2^5$ | 0.5m, $5^5$ | 5.0m, $10^5$ |
|------------------|-------------|-------------|-------------|
| Raw              | 85.1/85.4/84.3 | 92.7/93.1/92.7 | 97.3/98.2/97.6 |
| $\lambda = 0.1$ | 85.4/84.7/82.0 | 92.5/91.9/91.1 | 97.5/96.8/96.4 |
| $\lambda = 0.5$ | 84.7/84.3/82.9 | 92.4/91.9/91.0 | 97.2/96.7/96.1 |
| $\lambda = 2.5$ | 84.6/83.7/82.5 | 92.4/92.0/91.0 | 97.1/96.8/96.0 |

4.2. Utility retention

We measure the utility of NinjaDesc via two tasks: image matching and visual localization.

**Image matching.** We evaluate NinjaDesc based on SOSNet [68] with a set of different privacy parameter on the HPatches [5] benchmarks, which is shown in Fig. 5. NinjaDesc is comparable with SOSNet in mAP across all three tasks, especially for the verification and retrieval tasks. Also, higher privacy parameter $\lambda$ generally corresponds to lower mAP, as $\mathcal{L}_{util}$ becomes less dominant in Eqn. 9.

**Visual localization.** We evaluate NinjaDesc with three base descriptors - SOSNet [68], HardNet [37] and SIFT [33] on the Aachen-Day-Night v1.1 [57, 77] dataset using the Kapture [25] pipeline. We use AP-Gem [49] for retrieval and localize with the shortlist size of 20 and 50. The keypoint detector used is DoG [33]. Table 2 shows localization results. Again, we observe little drop in accuracy for NinjaDesc overall compared to the original base descriptors, ranging from low ($\lambda = 0.1$) to high ($\lambda = 2.5$) privacies. Comparing our results on HardNet and SIFT with Table 3 in Dusmanu et al. [16], NinjaDesc is noticeably better in retaining the visual localization accuracy of the base descriptors than the subspace descriptors in [16], e.g. drop in night is up to 30% for HardNet in [16] but $\approx 10\%$ for NinjaDesc.

Hence, the results on both image matching and visual localization tasks demonstrate that NinjaDesc is able to retain the majority of its utility w.r.t. to the base descriptors.

5. Ablation studies

Table 2 already hints that our proposed adversarial descriptor learning framework generalizes to several base descriptors in terms of retaining utility. In this section, we further investigate the generalizability of our method through additional experiments on different types of descriptors, inversion network architectures, and scene categories.

5.1. Generalization to different descriptors

We extend the same experiments from SOSNet [68] in Table 1 to include HardNet [37] and SIFT [33] as well. We

Note that in [9], only SSIM is reported, and we do not share the same train/validation/test split. Also, [9] uses the discriminator loss for training which we omit, and it leads to slight difference in SSIM.
Top. We show two matching images. Two rows of small images to the right of each of them are the reconstructions. The top & bottom rows are, respectively, the reconstructions from the raw descriptor and from NinjaDesc ($\lambda = 2.5$) associated with the base descriptor above. Bottom. We visualize the matches between the two images on raw descriptors vs. NinjaDesc ($\lambda = 2.5$) for each of the three base descriptors. Image credits: left — Tatyana Gladskih / stock.adobe.com; right — Urse Ovidiu (Wikimedia Commons, Public Domain).

Table 3. Qualitative performance of the descriptor inversion model on the MegaDepth [31] test split with three base descriptors and the corresponding NinjaDescs, varying in privacy parameter.

| Base Descriptor | SSIM ($\downarrow$) | Raw (w/o NinjaDesc) | NinjaDesc ($\lambda$) | Raw (w/o NinjaDesc) | NinjaDesc ($\lambda$) |
|----------------|---------------------|---------------------|-----------------------|---------------------|-----------------------|
| SOSNet         | 0.596               | 0.569               | 0.527                 | 0.484               | 0.385                 |
| HardNet        | 0.552               | 0.545               | 0.516                 | 0.399               | 0.349                 |
| SIFT           | 0.553               | 0.490               | 0.459                 | 0.395               | 0.362                 |

Table 4. Reconstruction results on MegaDepth [31]. We compare the UNet used in this work vs. a different architecture — UResNet.

| Arch. | UNet | UResNet |
|-------|------|---------|
| SOSNet | $\lambda = 1.0$ | $\lambda = 2.5$ | $\lambda = 1.0$ | $\lambda = 2.5$ |
| MAE ($\uparrow$) | 0.104 | 0.183 | 0.121 | 0.190 | 0.202 |
| SSIM ($\downarrow$) | 0.596 | 0.385 | 0.595 | 0.427 | 0.380 |
| PSNR ($\downarrow$) | 17.904 | 13.367 | 16.533 | 12.753 | 12.299 |

5.2. Generalization to different architectures

So far, all experiments are evaluated with the same architecture for the inversion model - the UNet [52]-based net-

work [9, 47]. To verify that NinjaDesc does not overfit to this specific architecture, we conduct a descriptor inversion attack using an inversion model with drastically different architecture, called UResNet, which has a ResNet50 [24] as the encoder backbone and residual decoder blocks. (See the supplementary material.) The results are shown in Table 4, which depicts only SSIM is slightly improved compared to UNet whereas MAE and PSNR remain relatively unaffected. This result illustrate that our proposed method is not limited by the architectures of the inversion model.

5.3. Content concealment on faces

We further show qualitative results on human faces using the Deepfake Detection Challenge (DFDC) [12] dataset. Fig. 7 presents the descriptor inversion result using the base descriptors (SOSNet [68]) as well as our NinjaDesc vary-
Figure 7. Qualitative reconstruction results on faces. Images are cropped frames sampled from videos in the DFDC [12] dataset.

ing in privacy parameter $\lambda$. Similar to what we observed in Fig. 4, we see progressing concealment of facial features as we increase $\lambda$ compared to the reconstruction on SOSNet.

6. Utility and privacy trade-off

We now describe two experiments we perform to further investigate the utility and privacy trade-off of NinjaDesc.

First, in Fig. 8a we evaluate the mean matching accuracy (MMA) of NinjaDesc at the highest privacy parameter $\lambda = 2.5$, for both HardNet [37] and SIFT [33], on the HPatches sequences [5] and compare that with the sub-hybrid lifting method by Dusmanu et al. [16] with low privacy level (dim. 2). Even at a higher privacy level, NinjaDesc significantly outperforms sub-hybrid lifting for both types of descriptors. For NinjaDesc, the drop in MMA w.r.t. to HardNet is also minimal, and even increases w.r.t. SIFT.

Second, in Fig. 8b we perform a detailed utility vs. privacy trade-off analysis on NinjaDesc for all three base descriptors. The $y$-axis is the average difference in NinjaDesc’s mAP across the three tasks in HPatches in Fig. 5, and the $x$-axis is the privacy measured by 1 - SSIM [9]. We plot the results varying the privacy parameter. For SOSNet and HardNet, the drop in utility ($<4\%$) is a magnitude less than the gain in privacy ($30\%$), indicating an optimal trade-off. Interestingly, for SIFT we see a net gain in utility for all $\lambda$ (positive values in the $y$-axis). This is due to the SOSNet-like utility training, improving the verification and retrieval of NinjaDesc beyond the handcrafted SIFT. Full HPatches results for HardNet and SIFT are in the supplementary.

7. Limitations

NinjaDesc only affects the descriptors, and not the keypoint locations. Therefore, it does not prevent inferring scene structures from the patterns of keypoint locations themselves [34, 64]. Also, some level of structure can still be revealed where keypoints are very dense, e.g. the venetian blinds in the second example of Fig. 7.

8. Conclusions

We introduced a novel adversarial learning framework for visual descriptors to prevent reconstructing original input image content from the descriptors. We experimentally validated that the obtained descriptors deteriorate the descriptor inversion quality with only marginal drop in utility using the standard benchmarks for descriptor matching. We also empirically demonstrated that we can control the trade-offs between utility and non-invertibility using our framework, by changing a single parameter that weights the adversarial loss. The ablation study using different types of visual descriptors and image reconstruction network architecture demonstrates the generalizability of our method. Our proposed pipeline can enhance the security of computer vision systems that use visual descriptors, and has great potential to be extended for other applications beyond local descriptor encoding. Our observation suggests that the visual descriptors contain more information than what is needed for matching, which is removed by the adversarial learning process. It opens up a new opportunity in general representation learning for obtaining representations with only necessary information for the target task to preserve privacy.
References

[1] Sameer Agarwal, Yasutaka Furukawa, Noah Snavely, Ian Simon, Brian Curless, Steven M Seitz, and Richard Szeliski. Building rime in a day. Communications of the ACM, 2011.

[2] Alexandre Alahi, Raphael Ortiz, and Pierre Vandergheynst. Freak: Fast retina keypoint. In CVPR, 2012.

[3] Relja Arandjelović, Petr Gronat, Akihiko Torii, Tomas Pajdla, and Josef Sivic. NetVLAD: CNN architecture for weakly supervised place recognition. In CVPR, 2016.

[4] Relja Arandjelović and Andrew Zisserman. DisLocation: Scalable descriptor distinctiveness for location recognition. In ACCV, 2014.

[5] Vassileios Balntas, Karel Lenc, Andrea Vedaldi, and Kristian Mikolajczyk. HPatches: A benchmark and evaluation of handcrafted and learned local descriptors. In CVPR, 2017.

[6] Michael Calonder, Vincent Lepetit, Christoph Strecha, and Pascal Fua. BRIEF: Binary robust independent elementary features. In ECCV, 2010.

[7] Kunal Chelani, Fredrik Kahl, and Torsten Sattler. How privacy-preserving are line clouds? Recovering scene details from 3d lines. In CVPR, 2021.

[8] Emmanuel d’Angelo, Laurent Jacques, Alexandre Alahi, and Pierre Vandergheynst. From bits to images: Inversion of local binary descriptors. TPAMI, 36(5):874–887, 2013.

[9] Deecka Dangwal, Vincent T. Lee, Hyo Jin Kim, Tianwei Shen, Meghan Cowan, Rajvi Shah, Caroline Trippel, Brandon Reagen, Timothy Sherwood, Vassileios Balntas, Armin Alaghi, and Eddy Ilg. Analysis and mitigations of reverse engineering attacks on local feature descriptors. In BMVC, 2021.

[10] Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li, and Li Fei-Fei. ImageNet: A large-scale hierarchical image database. In CVPR, 2009.

[11] Daniel DeTone, Tomasz Malisiewicz, and Andrew Rabinovich. SuperPoint: Self-supervised interest point detection and description. In CVPR Workshops, 2018.

[12] Brian Dollhansky, Joanna Bitton, Ben Pflaum, Jikuo Lu, Russ Howes, Menglin Wang, and Cristian Canton-Ferrer. The deepfake detection challenge dataset. CoRR, abs/2006.07397, 2020.

[13] Jing Dong, Erik Nelson, Vadim Indelman, Nathan Michael, and Frank Dellaert. Distributed real-time cooperative localization and mapping using an uncertainty-aware expectation maximization approach. In IJCAI, 2015.

[14] Alexey Dosovitskiy and Thomas Brox. Inverting visual representations with convolutional networks. In CVPR, 2016.

[15] Mihai Dusmanu, Ignacio Rocco, Tomas Pajdla, Marc Pollefeys, Josef Sivic, Akihiko Torii, and Torsten Sattler. D2-Net: A trainable cnn for joint detection and description of local features. In CVPR, 2019.

[16] Mihai Dusmanu, Johannes L Schönberger, Sudipta N Sinha, and Marc Pollefeys. Privacy-preserving visual feature descriptors through adversarial affine subspace embedding. In CVPR, 2021.

[17] Zekeriya Erkin, Martin Franz, Jorge Guajardo, Stefan Katzenbeisser, Inald Lagendijk, and Tomas Toft. Privacy-preserving face recognition. In International symposium on privacy enhancing technologies symposium, 2009.

[18] Marcel Geppert, Viktor Larsson, Pablo Speciale, Johannes L Schönberger, and Marc Pollefeys. Privacy preserving structure-from-motion. In ECCV, 2020.

[19] Marcel Geppert, Viktor Larsson, Pablo Speciale, Johannes L Schönberger, and Marc Pollefeys. Privacy preserving localization and mapping from uncalibrated cameras. In CVPR, 2021.

[20] Michael Goesle, Noah Snavely, Brian Curless, Hugues Hoppe, and Steven M. Seitz. Multi-view stereo for community photo collections. In CVPR, 2007.

[21] Ian J. Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial networks. In NIPS, 2014.

[22] Sam Hare, Amir Saffari, and Philip HS Torr. Efficient online structured output learning for keypoint-based object tracking. In CVPR, 2012.

[23] Christopher G Harris, Mike Stephens, et al. A combined corner and edge detector. In Alvey vision conference, volume 15, 1988.

[24] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In CVPR, 2016.

[25] Martin Humenberger, Yohann Cabon, Nicolas Guerin, Julien Morat, Jérôme Revaud, Philippe Rerole, Noé Pion, Cesar de Souza, Vincent Leroy, and Gabriela Csurka. Robust image retrieval-based visual localization using capture, 2020.

[26] Hervé Jégou, Matthijs Douze, and Cordelia Schmid. Hashing embedding and weak geometry consistency for large scale image search. In ECCV, 2008.

[27] Yuhe Jin, Dmytro Mishkin, Anastasiia Mishchuk, Jiri Matas, Pascal Fua, Kwang Moo Yi, and Eduard Trulls. Image matching across wide baselines: From paper to practice. IJCV, 2021.

[28] Hiroharu Kato and Tatsuya Harada. Image reconstruction from bag-of-visual-words. In CVPR, 2014.

[29] Diederik P Kingma and Jimmy Ba. Adam: A method for stochastic optimization. In ICLR, 2015.

[30] Alex Krizhevsky, Ilya Sutskever, and Geoffrey E Hinton. ImageNet classification with deep convolutional neural networks. Communications of the ACM, 2017.

[31] Zhengqi Li and Noah Snavely. MegaDepth: Learning single-view depth prediction from internet photos. In CVPR, 2018.

[32] Ce Liu, Jenny Yuen, and Antonio Torralba. SIFT flow: Dense correspondence across scenes and its applications. TPAMI, 2010.

[33] David G. Lowe. Distinctive image features from scale-invariant keypoints. In IJCV, 2004.

[34] Zixin Luo, Tianwei Shen, Lei Zhou, Jiahui Zhang, Yao Yao, Shiwei Li, Tian Fang, and Long Quan. ContextDesc: Local descriptor augmentation with cross-modality context. In CVPR, 2019.
Torsten Sattler. Long-term visual localization revisited. TPAMI, 2020.

[70] Carl Toft, Daniyar Turmukhambetov, Torsten Sattler, Fredrik Kahl, and Gabriel J Brostow. Single-image depth prediction makes feature matching easier. In ECCV, 2020.

[71] Giorgos Tolias, Yannis Avrithis, and Hervé Jégou. To aggregate or not to aggregate: Selective match kernels for image search. In ICCV, 2013.

[72] Giorgos Tolias, Tomas Jenicek, and Ondřej Chum. Learning and aggregating deep local descriptors for instance-level recognition. In ECCV, 2020.

[73] Carl Vondrick, Aditya Khosla, Tomasz Malisiewicz, and Antonio Torralba. Hoggles: Visualizing object detection features. In ICCV, 2013.

[74] Philippe Weinzaepfel, Hervé Jégou, and Patrick Pérez. Reconstructing an image from its local descriptors. In CVPR, 2011.

[75] Qizhe Xie, Zihang Dai, Yulun Du, Eduard Hovy, and Graham Neubig. Controllable invariance through adversarial feature learning. In NIPS, 2017.

[76] Ryo Yonetani, Vishnu Naresh Boddeti, Kris M Kitani, and Yoichi Sato. Privacy-preserving visual learning using doubly permuted homomorphic encryption. In ICCV, 2017.

[77] Zichao Zhang, Torsten Sattler, and Davide Scaramuzza. Reference pose generation for long-term visual localization via learned features and view synthesis. IJCV, 2020.

[78] Qiang Zhu, Mei-Chen Yeh, Kwang-Ting Cheng, and Shai Avidan. Fast human detection using a cascade of histograms of oriented gradients. In CVPR, 2006.
Supplementary material

We first provide a comparison of our NinjaDesc and the base descriptor on the 3D reconstruction task using SiM (Sec. A). Next, we report the full HPatches results using HardNet [37] and SIFT [33] as the base descriptors (Sec. B). In addition to our results on Aachen-Day-Night v1.1 in the main paper, we also provide our results on Aachen-Day-Night v1.0 (Sec. C). Finally, we illustrate the detailed architecture for the inverse models (Sec. D).

A. 3D Reconstruction

Table 5 shows a quantitative comparison of our content-concealing NinjaDesc and the base descriptor SOSNet [68] on the SiM reconstruction task using the landmarks dataset for local feature benchmarking [58]. As can be seen, decrease in the performance for our content-concealing NinjaDesc is only marginal for all metrics.

| Dataset                | Method      | Reg. images | Sparse points | Observations | Track length | Reproj. error |
|------------------------|-------------|-------------|---------------|--------------|--------------|---------------|
| South Building         | SOSNet      | 128 101,568 | 638,731       | 6.29         | 0.56         |
| 128 images             | NinjaDesc (1.0) | 105,780   | 652,869       | 6.17         | 0.56         |
|                        | NinjaDesc (2.5) | 105,961   | 653,449       | 6.17         | 0.56         |
| Madrid Metropolis      | SOSNet      | 572 95,733 | 672,836       | 7.03         | 0.62         |
| 1344 images            | NinjaDesc (1.0) | 566 94,374 | 668,148       | 7.08         | 0.64         |
|                        | NinjaDesc (2.5) | 564 94,104 | 667,387       | 7.09         | 0.63         |
| Gendarmenmarkt         | SOSNet      | 1076 246,503 | 1,660,694   | 6.74         | 0.74         |
| 1463 images            | NinjaDesc (1.0) | 1087 312,469 | 1,901,060   | 6.08         | 0.75         |
|                        | NinjaDesc (2.5) | 1030 340,144 | 1,871,726   | 5.50         | 0.77         |
| Tower of London        | SOSNet      | 825 200,447 | 1,733,994   | 8.65         | 0.62         |
| 1463 images            | NinjaDesc (1.0) | 797 198,767 | 1,727,785   | 8.69         | 0.62         |
|                        | NinjaDesc (2.5) | 837 218,888 | 1,792,908   | 8.19         | 0.64         |

Table 5. 3D reconstruction statistics on the local feature evaluation benchmark [58]. Number in parenthesis is the privacy parameter \( \lambda \).

B. Full HPatches results for HardNet and SIFT

Figure 9 illustrates our full evaluation results on HPatches using HardNet [37] and SIFT [33] as the base descriptors for NinjaDesc, in addition to the results using SOSNet [68] as the 5 encealing/down-sampling blocks, except for \( \text{conv}_2 \) we remove the MaxPool2d so that each encoding block corresponds to a 1/2 down-sampling in resolution. Since ResNet50 takes in RGB image as input (which has shape of \( 3 \times h \times w \), whereas the sparse feature maps are of shape \( 128 \times h \times w \)), we pre-process the input with 4 additional basic residual blocks denoted by \( \text{res}_n \) in Figure 11. The up-sampling decoder blocks (denoted by \( \text{up}_n \)) are also residual blocks with an addition in-

C. Evaluation on Aachen-Day-Night v1.0

In Table 2 of the main paper, we report the result of NinjaDesc on Aachen-Day-Night v1.1 dataset. The v1.1 is updated with more accurate ground-truths compared to the older v1.0. Because Dusmanu et al. [16] performed evaluation on the v1.0, we also provide our results on v1.0 in Table 6 for better comparison.

| Query NNs Method | accuracy @ Thresholds (%) |
|------------------|---------------------------|
| Base Desc | SOS / Hard / SIFT | SOS / Hard / SIFT | SOS / Hard / SIFT |
| Raw | 85.1/84.7/84.3 | 92.7/93.1/92.7 | 97.3/98.2/97.6 |
| 20 | \( \lambda = 0.1 \) | 85.4/84.7/84.3 | 92.5/91.9/91.1 | 97.5/96.8/96.4 |
| 50 | \( \lambda = 1.0 \) | 84.7/84.3/82.9 | 92.4/91.9/91.0 | 97.6/96.7/96.1 |
| 100 | \( \lambda = 2.5 \) | 84.6/83.7/82.5 | 92.4/90.2/90.1 | 97.1/96.8/96.0 |
| Day (824) Raw | 85.9/86.8/86.0 | 92.5/93.7/94.1 | 97.3/98.1/98.2 |
| 20 | \( \lambda = 0.1 \) | 85.2/85.2/84.2 | 92.2/92.4/91.4 | 97.1/97.1/96.6 |
| 50 | \( \lambda = 1.0 \) | 84.7/87.5/83.4 | 92.2/92.6/91.6 | 97.2/96.7/96.7 |
| 100 | \( \lambda = 2.5 \) | 85.6/85.3/83.6 | 92.7/91.7/91.1 | 97.3/96.8/96.2 |
| Night (98) Raw | 51.0/57.2/55.1 | 65.3/68.4/67.3 | 70.4/76.5/74.5 |
| 20 | \( \lambda = 0.1 \) | 51.0/45.9/49.5 | 62.2/56.1/54.1 | 68.4/62.2/63.3 |
| 50 | \( \lambda = 1.0 \) | 50.0/43.9/44.9 | 62.2/54.1/56.1 | 66.3/62.2/64.3 |
| 100 | \( \lambda = 2.5 \) | 48.0/44.4/44.9 | 58.2/52.9/52.0 | 65.3/65.3/62.2 |

Table 6. Visual localization results on Aachen-Day-Night v1.0 [57]. ‘Raw’ corresponds to the base descriptor in each column, followed by three \( \lambda \) values (0.1, 1.0, 2.5) for NinjaDesc.

D. Detailed architectures of the descriptor inversion models

UNet. The architecture of the UNet-based descriptor inversion model, which is also used in [9, 47], is shown in Figure 10.

UResNet. Figure 11 illustrates the architecture of the descriptor inversion model based on UResNet used for the ablation study in the Section 5.2 of the main paper. The overall “U” shape of UResNet is similar to UNet, but each convolution block is drastically different. We use the 5 stages of ResNet50 [24] (pretrained on ImageNet [10]) \{conv1, conv2_x, conv3_x, conv4_x, conv4_x\} as the 5 encoding/down-sampling blocks, except for \( \text{conv}_2 \) we remove the MaxPool2d so that each encoding block corresponds to 1/2 down-sampling in resolution. Since ResNet50 takes in RGB image as input (which has shape of \( 3 \times h \times w \), whereas the sparse feature maps are of shape \( 128 \times h \times w \)), we pre-process the input with 4 additional basic residual blocks denoted by \( \text{res}_n \) in Figure 11. The up-sampling decoder blocks (denoted by \( \text{up}_n \)) are also residual blocks with an addition in-
Figure 9. HPatches evaluation results. For each base descriptor (HardNet [37] and SIFT [33]), we compare with NinjaDesc, with 5 different levels of privacy parameter $\lambda$ (indicated by the number in parenthesis). All results are from models trained on the *liberty* subset of the UBC patches [20] dataset, apart from SIFT which is handcrafted, and we use the Kornia [51] GPU implementation evaluated on $32 \times 32$ patches.

put up-sampling layer using bilinear interpolation. In contrast to UNet, the skip connections in our UResNet are performed by additions, rather than concatenations.
Figure 10. UNet Architecture.

Figure 11. UResNet Architecture.