

ReFace: Real-time Adversarial Attacks on Face Recognition Systems

Shehzeen Hussain^{*1}, Todd Huster^{*2}, Chris Mesterharm², Paarth Neekhara¹, Kevin An¹, Malhar Jere,
Harshvardhan Sikka³, and Farinaz Koushanfar¹

¹ UC San Diego, La Jolla, CA 92093, USA {ssh028,pneekhar,k1an,fkoushanfar}@eng.ucsd.edu

² Peraton Labs, Basking Ridge, NJ 07920, USA {thuster,jmesterharm}@peratonlabs.com

³ Georgia Institute of Technology, Atlanta, Georgia 30332, USA
harshsikka@gatech.edu

Abstract. Deep neural network based face recognition models have been shown to be vulnerable to adversarial examples. However, many of the past attacks require the adversary to solve an input-dependent optimization problem using gradient descent which makes the attack impractical in real-time. These adversarial examples are also tightly coupled to the attacked model and are not as successful in transferring to different models. In this work, we propose ReFace, a real-time, highly-transferable attack on face recognition models based on Adversarial Transformation Networks (ATNs). ATNs model adversarial example generation as a feed-forward neural network. We find that the white-box attack success rate of a pure U-Net ATN falls substantially short of gradient-based attacks like PGD on large face recognition datasets. We therefore propose a new architecture for ATNs that closes this gap while maintaining a 10000× speedup over PGD. Furthermore, we find that at a given perturbation magnitude, our ATN adversarial perturbations are more effective in transferring to new face recognition models than PGD. ReFace attacks can successfully deceive commercial face recognition services in a transfer attack setting and reduce face identification accuracy from 82% to 16.4% for AWS SearchFaces API and Azure face verification accuracy from 91% to 50.1%.

Keywords: Adversarial machine learning, adversarial attacks, deep learning, security, face recognition

1 Introduction

Face recognition and verification systems are widely used for identity authentication in government surveillance, military applications, public security settings such as airports, hotels, banks as well as smartphones to unlock applications. Over recent years, Convolutional Neural Networks (CNNs) have achieved state-of-the-art results on several face recognition and verification benchmarks outperforming traditional computer vision algorithms that rely on hand engineered features. With the widespread adoption of face recognition models in surveillance and other security sensitive applications, careful vulnerability analysis is imperative to ensure their safe deployment.

Several works have shown that deep neural networks (DNNs) are vulnerable to adversarial examples, causing the model to make an incorrect prediction with higher confidence [4,9,13,20,25]. Particularly, past attacks [10,31] on face recognition systems have garnered immense media attention [1,2] by utilizing projected gradient descent (PGD) [23] based approaches to achieve high fooling success rates. However, designing such adversarial examples requires the adversary to solve an optimization problem for each input. This makes the attack impractical in real-time since the adversary would need to re-solve the data-dependent optimization problem from scratch for every new input.

To generate adversarial attacks against classification systems in real-time, some past works, such as Adversarial Transformation Networks (ATNs) [5], have attempted to learn a perturbation function with a neural network. ATNs are encoder-decoder neural networks that are trained to generate an adversarial image directly from an input image without having to perform multiple forward-backward passes on the victim classification model during inference, thereby making the attack possible in real time. However, ATNs have only been explored for classification tasks. The training objective studied thus far for an ATN is to push the classifier's

^{*} Equal contribution

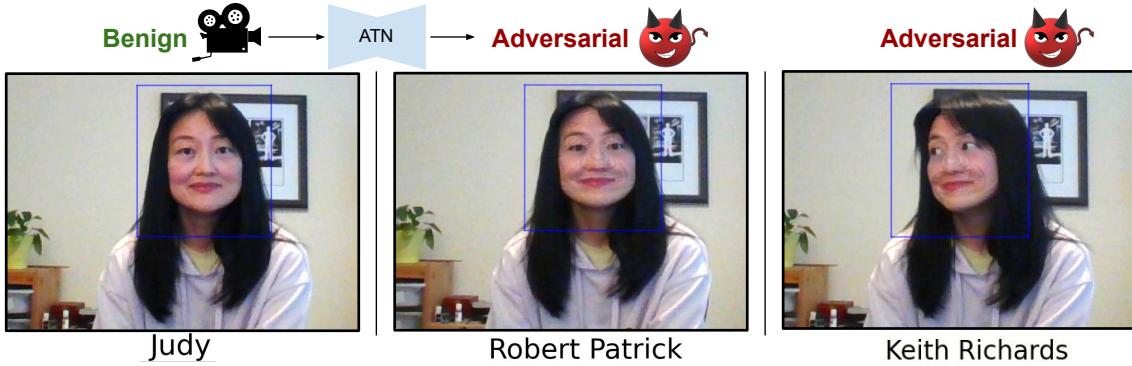


Fig. 1. Demonstration of ReFace attack in real-time. Sample screenshots captured from attack demo video posted on our project webpage.

output outside the decision boundary of the correct class. Unlike a classification model, where model outputs are class probabilities, the output space of a typical face recognition system is an embedding vector. A face recognition system is trained to cluster the embeddings of the same identity together in the embedding space while ensuring they are well separated from the embeddings of other identities. Therefore when attacking such a setup, the attack objective requires the adversary to target the embedding space rather than the decision boundaries of the classifier.

To perform attacks on face recognition models, we first develop training objectives that target the embedding space of face recognition models and optimize metrics that degrade the identification and verification performance of such models. To minimize perceptibility of our perturbations, we incorporate Learned Perceptual Image Patch Similarity L_{pips} perceptual loss [36] in addition to the L_∞ constraint during training. Next, to perform real-time attacks, we design a new ATN based on the U-net [29] architecture, since U-nets have been notably effective in many prior image-to-image translation tasks [18,17]. We find that while a U-net based ATN can generate real-time adversarial examples, the attack performance falls short as compared to per-image gradient based attacks such as PGD [23] at the same magnitude of adversarial perturbation. This is because gradient-based attacks generate highly tailored adversarial examples that are optimized on a single image. We address the performance gap between ATN and PGD attacks through neural architectural improvements to our ATN model which we describe in Section 3.4.

Having bridged the gap with gradient based attacks on seen victim models, we evaluate the transferability of our adversarial samples to unseen models. Since ATNs are trained on a diverse set of images, we find that perturbations generated from an ATN are more transferable to unseen architectures as compared to per-input PGD attack, while being much faster to compute. To further improve our attack transferability, we adapt our ATN training framework to target an ensemble of face recognition models with various backbone architectures. Our best ATN attacks on unseen models successfully reduce the performance of face recognition models to the level of random guessing or worse. We present a demo video of our attack in real-time on our project webpage⁴ with sample images presented in Figure 1. Finally, we demonstrate our attack effectiveness against cloud-hosted face recognition APIs in a complete black-box setting. The technical contributions of our work are as follows:

- We propose a real-time attack framework to study the robustness of face recognition systems and demonstrate that our ATNs can synthesize adversarial examples several orders of magnitude faster than existing attacks on face recognition systems while achieving comparable attack success metrics as past works. To the best of our knowledge this is the first real-time attack on face recognition systems, in contrast to previous works which perform gradient based attacks or study real-time attack only in the classification domain.
- We bridge the performance gap between real-time ATN attacks and PGD attacks by developing a Residual U-net architecture that allows us to effectively increase the capacity of the ATN (Section 3.4). Our ResU-

⁴ <https://refaceattack.github.io/>

Net ATN approaches PGD performance in white-box attacks and outperforms PGD on black-box transfer attacks.

- We develop and release a benchmarking library for face recognition models (Section 4.1)⁵. This allows us to evaluate our attacks on diverse set of architectures and loss functions. This library may be used to develop more robust face recognition models and to provide benchmarks of models’ performance in an adversarial setting.
- We demonstrate the effectiveness of our real-time attacks on commercial face recognition services such as Amazon Face Rekognition and Microsoft Azure Face. Our attacks reduce face identification accuracy from 82% to 16.4% for AWS SearchFaces and face verification accuracy from 91% to 50.1% for Microsoft Azure.

2 Related Work

An adversarial example is an input sample which has been perturbed in a way that is intended to cause misclassification by a victim machine learning model [6,35]. Prior work on attacks have demonstrated that adversarial examples can circumvent state-of-the-art image classification models while remaining indistinguishable from benign images for humans [9,13,23,16,15,25,26,32]. However many of these works are gradient based attacks, which cannot be performed in real-time. To address this limitation, the authors of UAPs [24] demonstrated that there exist universal *input-agnostic* perturbations which when added to any image will cause the image to be misclassified by a victim network. The existence of such perturbations poses a threat to machine learning models in practical settings since the adversary may simply add the same pre-computed perturbation to a new image and cause misclassification in real-time. Also addressing the real-time challenge, the authors of [5] designed Adversarial Transformation Networks (ATNs) that follow an encoder-decoder architecture and output an adversarial perturbation for each input image, without having to compute gradients from the victim classification model during inference [5]. Unlike UAPs, ATNs generate input-specific perturbations. However these ATN attacks are specific to image classification tasks and cannot be directly used to attack face recognition models that use task-specific model and loss functions as opposed to the standard cross-entropy loss used by classifiers.

Studies on generating adversarial examples for face recognition models are relatively fewer in literature as compared to image classification attacks. The authors of [28] attempt to target face “classification” networks which operate differently from face recognition networks that perform face verification and identification. Prior works such as [12,30,31,10] generate adversarial examples for face recognition systems by optimizing the perturbation for each image using white-box access to a face-recognition model. One such attack [10] demonstrates that it is possible to generate adversarial faces by optimizing in the model embedding space using PGD [23] and CW [9] attack, however reports an attack run-time from 6 seconds to 373 seconds per image while using 2 GPUs. Another gradient based attack Lowkey [11] generates image-specific adversarial samples for face recognition models and demonstrates their transferability to public cloud provider APIs, however reports an attack run-time of 32 seconds per image. To generate adversarial examples in black-box settings, the authors of [12] utilize an evolutionary optimization technique, but require at least 1,000 queries to the target face recognition system before a realistic adversarial face can be synthesized. Similarly, the more recently proposed black-box attack by [7] on face recognition systems requires at least 1700 queries to generate successful attacks. The time for generating adversarial examples using these techniques can potentially bottleneck real-time image upload making the attacks impractical for deployment. In contrast, we propose a framework to adversarially modify query images in real-time, such that the performance of face recognition models deteriorate significantly in both white-box and transfer based black-box attack settings.

3 Methodology

3.1 Victim Models

A typical face recognition pipeline first detects and crops faces. Next, they map each cropped image x to an embedding vector y using $F : x \mapsto y$. Typically, such models are trained on a dataset of facial images and identity labels, with the objective of clustering embeddings of images from the same identity together and ensuring

⁵ Model test bed to be released upon publication

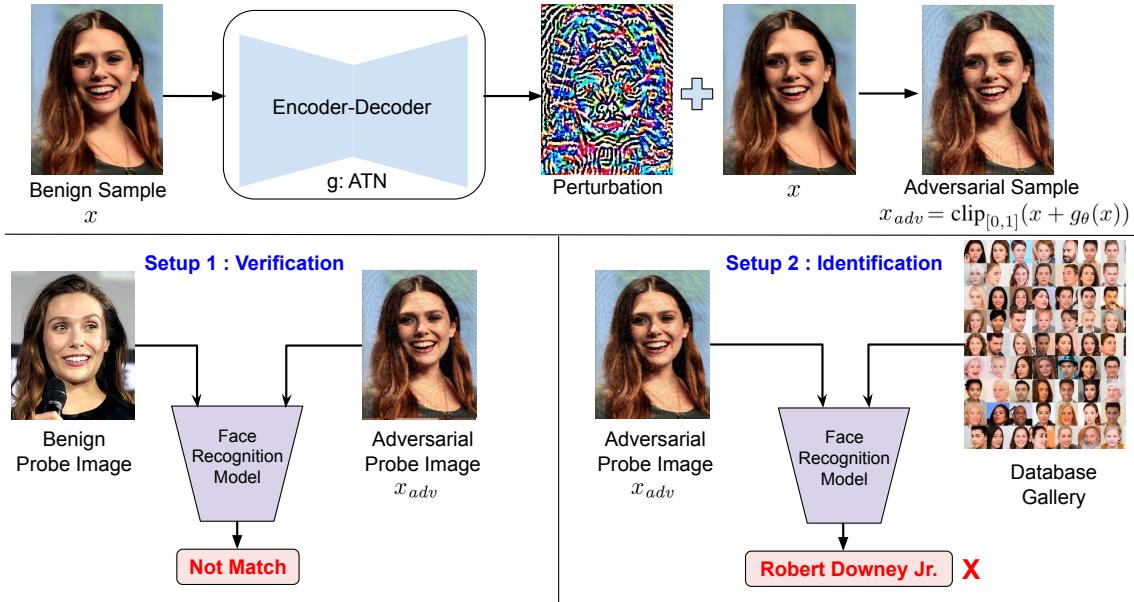


Fig. 2. Overview of ReFace adversarial perturbation generator (top) and attack application on face verification and identification systems (bottom). Photo credit: Gage Skidmore

separability between embeddings of images from different identities. State-of-the-art face recognition models are commonly trained with objectives that effectively optimize a cosine distance metric e.g. SphereFace [22] or DeepID [33] loss. During inference, a face recognition model can be used for one of the following goals:

1. **Verification** - A face recognition model can be used to verify whether two images belong to the same person or not. In this setting, the model compares the embeddings of two probe images and reports a match if the distance between the embeddings of the two models is below a certain threshold.
2. **Identification** - In this setting, the face recognition system tries to associate a person with an identity from a set of identities in *gallery images* stored in the system's database. When presented with a *probe image*, the system compares the embedding of the probe image with the gallery images to find the closest matching neighbour in the gallery and determine the identity of the probe image.

In our work, we attack CNN-based face recognition models in real time and assess the success rate against both of the above goals. To simplify experimentation, we do not include the detection and cropping step in our attacks pipeline. Instead we use the pre-cropped images provided by standard datasets.

3.2 Problem Formulation

We design a perturbation generator that operates in real-time and finds a quasi-imperceptible adversarial perturbation for an input image, which when added to the input causes mis-prediction of the embedding vector thereby degrading the verification and identification performance of the face recognition model. When attacking a *face verification* system, we adversarially perturb one of the two probe images. In this attack setting, our goal is to reduce the true recall rate of the verification system (performance on positive pairs). When attacking a *face identification* system, we assume the probe images have been adversarially perturbed while the dataset of gallery images is benign. In this attack setting, our goal is to lower the recognition rate of the face identification system.

To achieve the above objectives, we train a perturbation generator g_θ , parameterized by θ , which takes as input an image x and generates an adversarial perturbation $g_\theta(x)$ that can be added to x to synthesize an adversarial example x_{adv} . The optimization objective of g_θ is to maximize the cosine distance the embeddings of the adversarial and original image, while constraining the amount of the perturbation added to the image. This is different from the objective for fooling classification systems, where the commonly used objective for

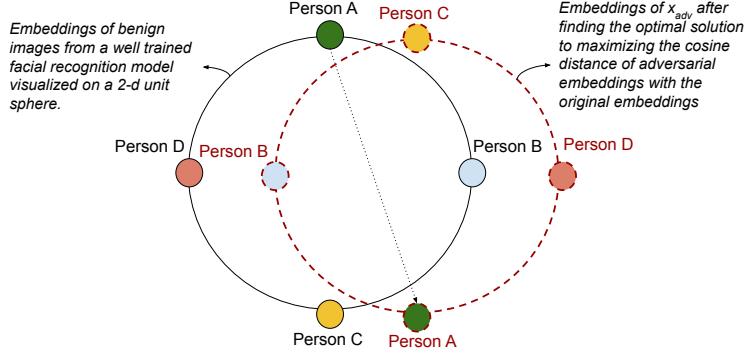


Fig. 3. Visualizing the optimum solution to our attack objective: Our attack objective pushes the originally predicted embedding vectors to the opposite end of the unit sphere thereby hampering the performance of the face-recognition model.

untargeted attacks is to maximize the cross-entropy loss with the correct label. L_p norm is a widely used distance metric for measuring the distortion between the original and adversarial inputs. Prior works [13] recommend constraining the maximum distortion of any individual pixel using the L_∞ norm. To further reduce the perceptibility of the perturbation we incorporate L_{pips} [36] loss during training. L_{pips} distance measures the visual similarity between two images by comparing the embeddings from a pre-trained CNN model.

Mathematically, our attack objective is as follows:

$$\begin{aligned} \forall_{x \in X} \text{ maximize } & [d(F(x_{adv}), F(x)) - \lambda L_{pips}(x_{adv}, x)] \\ \text{where } x_{adv} = & \text{clip}_{[0,1]}(x + g_\theta(x)) \\ \text{s.t } & \|g_\theta(x)\|_\infty < \epsilon \end{aligned} \quad (1)$$

where $d(F(x_{adv}), F(x))$ is the cosine distance between embeddings of the adversarial and original image and λ is the loss coefficient for L_{pips} . In Figure 3 we illustrate how an optimum solution to the above problem of maximizing the cosine distance completely degrades the performance of a face recognition model. A visualization of such embedding clusters for a hypothetical case of four individuals on a 2-D unit sphere is shown on the left in Figure 3. If we were to find the optimum solution to our attack objective in an unbounded attack setting, the embeddings clusters for adversarial images will move to the opposite end of the unit sphere (to maximize the cosine distance). This clearly results in hampering both verification and identification performance of the model since the embeddings of benign and adversarial examples are completely rotated to the opposite ends in the unit sphere.

In our work, we model g_θ as a neural encoder-decoder architecture called an Adversarial Transformation Network (ATN) (Section 3.3).

3.3 ATN: Adversarial Transformation Network

An ATN is a neural network trained to produce adversarial images, with the form $g_\theta : \mathcal{X} \rightarrow \mathcal{X}$. Since the network only needs one forward pass to compute the perturbation, it is less expensive than an iterative gradient-based optimization procedure. We obtain an adversarial image from a benign image using the neural network N_θ as follows:

$$g_\theta(x) = \epsilon \cdot \tanh(N_\theta(x)) \quad (2)$$

With this formulation we enforce the constraint $\|x_{adv} - x\|_\infty < \epsilon$ since the output of \tanh is bounded between $[-1, 1]$.

Algorithm 1 Ensemble attack training procedure

Inputs: Victim Models $\mathbb{F} = F_1, \dots, F_n$, image dataset X
Output: Perturbation engine (g_θ) parameters θ
HyperParams: Learning rate α , L_∞ bound ϵ , L_{pips} loss coefficient λ

Initialize ATN: N_θ
Batch training images: $X_{batched} \leftarrow Batch(X)$
for epoch in 0 to N_{epochs} **do**
 for x in $X_{batched}$ **do**
 $x_{adv} \leftarrow \text{clip}_{[0,1]}(x + \epsilon \cdot \tanh(N_\theta(x)))$
 loss $\leftarrow 0$
 for F_i in F **do**
 $loss \leftarrow loss + (-d(F_i(x), F_i(x_{adv})))$
 end for
 $loss \leftarrow loss/\text{len}(F)$
 $loss \leftarrow loss + \lambda L_{pips}(x_{adv}, x)$
 $\theta \leftarrow \theta - \alpha \cdot \nabla_\theta(loss)$
 end for
end for
return θ

We train the ATN to generate adversarial examples using the procedure described in Algorithm 1. Our ATN can be trained to target one or more face recognition models in the model set \mathbb{F} . During each mini-batch iteration, we generate a batch of adversarial images from the ATN and compute the cosine distance between embeddings of benign and adversarial images. We accumulate the loss for all models in the set \mathbb{F} and can optionally add the L_{pips} loss to minimize the perceptibility of the adversarial perturbation. Finally, we backpropagate through all models in the set \mathbb{F} to compute the gradient of the loss with respect to the parameters θ of the ATN and update the ATN parameters using mini-batch gradient descent with a learning rate α . Targeting an ensemble of face recognition models during training can result in more transferable adversarial attacks. In our experiments, we verify this hypothesis and demonstrate that ATNs trained to target an ensemble of models result in better transferability to unseen models.

3.4 The search for an effective ATN architecture

The input and output domains of the ATN have the same spatial dimension, so a logical choice for the network architecture is a U-net [29]. U-nets are commonly used for several image-to-image translation problems. The architecture consists of several down-sampling layers followed by an equal number of up-sampling layers. The feature maps from the down-sampling layers have skip connections that are concatenated to the up-sampling layers with matching resolution. Previous work with ATNs used different architectures, but in our preliminary experiments, we found that U-nets were far more effective than alternate architectures at the same level of perturbation.

However, we still found that there was a large gap between a U-net based ATN and an iterative gradient-based white-box attack, *even on the training data*. This is illustrated in Figure 5 in our experiments comparing PGD-30 (i.e., 30 iterations of PGD) to the U-net ATN. From the universal approximation theorem [27], a neural network could in principle represent a close approximation of the PGD-30 function. As this neural network would have lower training loss than the U-net ATN, it appears that this architecture is *underfitting*. We therefore explored ways to add capacity to the ATN. We found that adding layers and making the layers wider both led to small gains in performance with diminishing returns.

One feature of the U-net is that every layer changes the spatial resolution. The deeper layers of the U-net necessarily operate at very low spatial resolutions. Intuitively, it may be useful to be able to express complex hierarchical functions at higher resolutions. We developed a new Residual U-net architecture, illustrated in Figure 4, that replaces individual convolution and transpose convolution layers in a U-net with groups of residual blocks. We use 2-layer pre-activation blocks with ReLU and batch normalization. One skip connection per downsample is carried over to the decoder, which allows arbitrary numbers of residual blocks at each step.

We denote the number of blocks in each group as a vectors \mathbf{E} and \mathbf{D} for the encoder and decoder, respectively. While similar architectures have been proposed in the past [3,21], they are not widely used and have not been used in adversarial perturbation literature.

We found that adding layers in this architecture was considerably more effective than in the pure U-net ATN. We performed an architecture search to find an effective balance between computational cost and attack effectiveness. The optimal architecture from this process had five downsampling steps with $\mathbf{E} = [1, 1, 2, 3, 5]$ and $\mathbf{D} = [1, 1, 1, 1, 1]$. We use a base width of 64 channels and double the width at each downsample step except for the last. Using this ResU-net architecture, the ATN approached the performance of PGD-30 (plotted in Figure 5a) with roughly $10,000 \times$ less run-time. We refer the readers to the code-base included in our supplementary material for the precise model implementation.

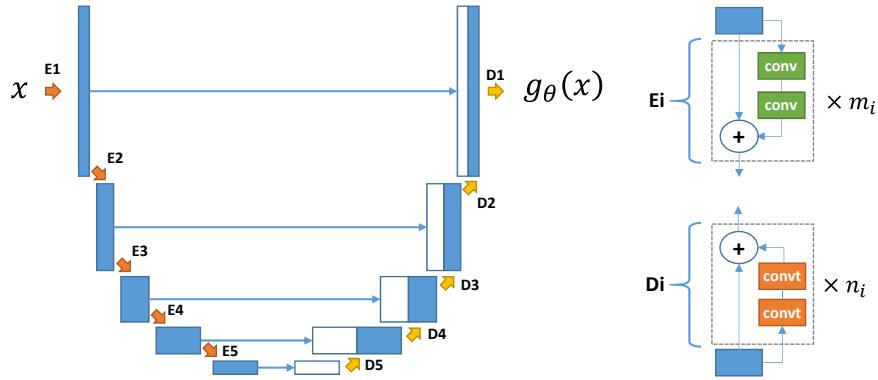


Fig. 4. Residual U-net architecture: We replace the strided convolutions and transposed convolutions in the U-Net architecture with residual blocks. Each residual block contains multiple convolutions (in the encoder) or transposed convolution (in the decoder) layers.

4 Experiments

4.1 Dataset and Models

We developed a benchmarking framework to evaluate both white-box and transfer attack performance of adversarial examples generated using our ATNs. Our experiments are designed to examine how factors such as network architecture, training loss functions, and random initialization affect the transferability of attacks. We used two main CNN architectures for the face recognition models: pre-activation ResNet [14] and Inception-v4 [34]. Within these architectures, we varied the number of blocks leading to networks ranging from 22 to 118 layers which were trained with two different loss functions: DeepID [33] and SphereFace [22]. The face recognition models are trained on the training partition of the VGGFace2 dataset [8]. We start with the standard crops provided by each dataset and perform random resized cropping for data augmentation during training.

These models are listed in Table 1 and are used to train our ATNs. The model sets include both single and ensemble face recognition models for each architecture to test the effectiveness of ensemble attacks on unseen models. For ensemble models, the reported metrics are averaged over all individual models in the ensemble. We split the VGGFace2 validation set into two equal partitions with disjoint identities. We train our ATNs on the first partition and evaluate them on the second.

4.2 Evaluation Metrics

We evaluate the performance of face recognition models on both verification and identification tasks with the metrics described below.

Name	Architecture	Networks		Verification		Identification
		# Models	Loss	V-AUC	V-Acc.	R1-Acc.
RN-SF-1	ResNet	1	SphereFace	0.99	95.2	84.4
RN-DID-1	ResNet	1	DeepID	0.98	93.3	78.0
IN-SF-1	InceptionNet	1	SphereFace	0.99	94.4	78.5
RN-SF-6	ResNet	6	SphereFace	0.99	94.3	82.0
RN-DID-6	ResNet	6	DeepID	0.98	93.0	77.4
IN-SF-4	InceptionNet	4	SphereFace	0.99	94.4	78.9

Table 1. Victim model sets used for conducting our attack evaluations. Experiments are conducted on both single and ensemble model sets. The verification and identification metrics are averages over the whole model set reported on the *clean* unperturbed VGGFace2 test set.

Face Verification Metrics: For each identity in the test set, we prepare all possible pairs of distinct images that have the same identity. To keep our problem balanced, we randomly sample an equal number of non-matching pairs. On the test set of VGGFace2, this creates a total of 917,692 verification tests where half have a pair of images with matching identities (positive labels) and half have different identities (negative labels). Given this binary classification problem, we report the following metrics:

1. *Verification AUC (V-AUC)*: We use the cosine distance between the embedding of the two images along with the verification label to generate a Receiver Operating Characteristic curve (ROC). Our metric is the standard area under the ROC curve (AUC).

2. *Verification Accuracy (V-Acc.)*: To determine the accuracy, we need a threshold for the cosine distance, across which the example is labelled positive or negative. For each model, we set this to *equal error rate* threshold of the model on the (clean) VGGFace2 validation set.

Face Identification Metric: We use the VGGFace2 test set to create a random gallery with 100 unique identities. For each of these 100 identities, we select a probe image with one of the identities appearing in the gallery and compute its distance to each image in the gallery. This creates 100 identification tests. We repeat this gallery test on 1000 random galleries to create a total of 100,000 identification tests. When evaluating attacks, we perturb the probe image and leave the gallery unmodified. We report the *Rank-1 Accuracy (R-1)*, which is the percentage of tests where the image in the gallery with the minimum distance to the probe image has the same identity as the probe image.

4.3 Baseline Attacks

We compare the effectiveness of ATN attacks against three alternate attacks:

1. Universal Adversarial Perturbations (UAP): UAP is a single input-agnostic perturbation vector that can be added to all images to fool the victim models. UAP can be formulated as a simplified ATN where the ATN formulation reduces to : $g_\theta(x) = \epsilon \cdot \tanh(\theta_{h \times w \times c})$. That is, instead of modeling ATN as a neural network, the ATN is modelled using a perturbation vector $\theta_{h \times w \times c}$ which is trained using the same procedure given by Algorithm 1.
2. Fast Gradient Sign Method (FGSM): FGSM [13] attack obtains an adversarial example for an image by obtaining the gradient of the optimization objective with respect to the image and then perturbing the image in the direction of the gradient with step size ϵ . That is, $x_{adv} = clip_{[0,1]}(x + \epsilon \cdot sign(\nabla_x L(x)))$ where $L(x)$ is the optimization objective given by Equation 1.
3. Projected Gradient Descent (PGD): PGD [23] attack is a multi-step iterative variant of the FGSM attack. Unlike ATNs and UAPs, PGD attack requires several forward and backward passes through a victim face-recognition model to find an adversarial perturbation that is highly optimized for a single image. We perform PGD attack as a baseline because it has been commonly adopted by past attacks such as Fawkes [31], Face-Off [10] and achieves highest white-box attack success rates.

5 Results

We train six ATN models each targeting one of the model sets listed in Table 1. The ATNs are trained using mini-batch gradient descent with a batch size 32 for 500K iterations using Adam optimizer [19] with a learning rate $2e-4$. Our primary evaluation is conducted using the ResU-Net ATN architecture described in Section 3.4 at max L_∞ distortion $\epsilon = 0.03$ in $[0, 1]$ pixel scale. We present the white-box and transfer attack results of our primary evaluation in Table 2. Additionally, we present the results and comparisons for the pure U-Net architecture in Section 5.2 and comparison against alternate attacks at $\epsilon = [0.01, 0.02, 0.03]$ in Figure 5.

			Single Defender Models			Ensemble Defender Models		
			RN-SF-1	RN-DID-1	IN-SF-1	RN-SF-6	RN-DID-6	IN-SF-4
Verification AUC	No Attack	Clean	0.99	0.98	0.99	0.99	0.98	0.99
	<i>Single Model Attack</i>	RN-SF-1	0.03	0.59	0.87	0.59	0.71	0.89
		RN-DID-1	0.58	0.04	0.88	0.64	0.55	0.88
		IN-SF-1	0.75	0.77	0.03	0.77	0.79	0.54
	<i>Ensemble Model Attack</i>	RN-SF-6	0.06	0.12	0.35	0.07	0.14	0.37
		RN-DID-6	0.13	0.07	0.45	0.10	0.08	0.44
		IN-SF-4	0.37	0.43	0.05	0.31	0.43	0.05
Verification Accuracy	No Attack	Clean	95.2%	93.3%	94.4%	94.3%	93.3%	94.4%
	<i>Single Model Attack</i>	RN-SF-1	48.8%	59.3%	67.9%	64.3%	65.5%	82.7%
		RN-DID-1	62.5%	49.4%	82.3%	64.4%	60.6%	81.6%
		IN-SF-1	71.2%	68.9%	48.4%	70.9%	70.0%	63.6%
	<i>Ensemble Model Attack</i>	RN-SF-6	48.4%	48.5%	53.4%	48.2%	48.3%	53.5%
		RN-DID-6	48.8%	48.7%	57.2%	48.1%	48.6%	56.4%
		IN-SF-4	50.8%	51.0%	47.9%	49.5%	50.9%	48.0%
Rank-1 Accuracy	No Attack	Clean	84.4%	78.0%	78.5%	82.0%	77.4%	78.9%
	<i>Single Model Attack</i>	RN-SF-1	0.0%	12.6%	43.5%	18.0%	19.4%	44.0%
		RN-DID-1	16.4%	0.0%	43.1%	17.4%	12.6%	41.0%
		IN-SF-1	30.3%	26.1%	0.0%	26.7%	25.6%	16.4%
	<i>Ensemble Model Attack</i>	RN-SF-6	0.1%	0.2%	5.3%	0.1%	0.2%	5.1%
		RN-DID-6	0.7%	0.1%	8.6%	0.3%	0.0%	7.6%
		IN-SF-4	2.2%	2.2%	0.0%	1.0%	2.0%	0.0%

Table 2. White-box and transfer attack results of ATN attack at $\epsilon = 0.03$. A lower value for all three metrics indicates a more successful attack. The diagonal entries in each of the three tables represents a white-box attack while all other entries represent a transfer (black-box) attack.

5.1 Single Model Attack vs Ensemble Attack

Aversarial perturbations trained on an ensemble of victim models exhibit better transferability across model architectures than those trained on a single model. That is, the attack success metrics on unseen models for ATNs trained on ensemble models (RN-SF-6, RN-DID-6 and IN-SF-4) are significantly better than ATNs trained on single models (RN-SF-1, RN-DID-1 and IN-SF-1 respectively). The only difference amongst the models in an ensemble is their weight initialization. It is interesting to note that this difference in weight initialization offers enough variance in the model set to train significantly more generalizable perturbations, at the same level of distortion as compared to the single-model attacks.

5.2 PGD vs. ATN

We compare the effectiveness of ATNs and PGD on both seen and unseen models. We optimize PGD-30 and ATN attacks on the same surrogate models and perform the attack on a random subset of 10,000 images

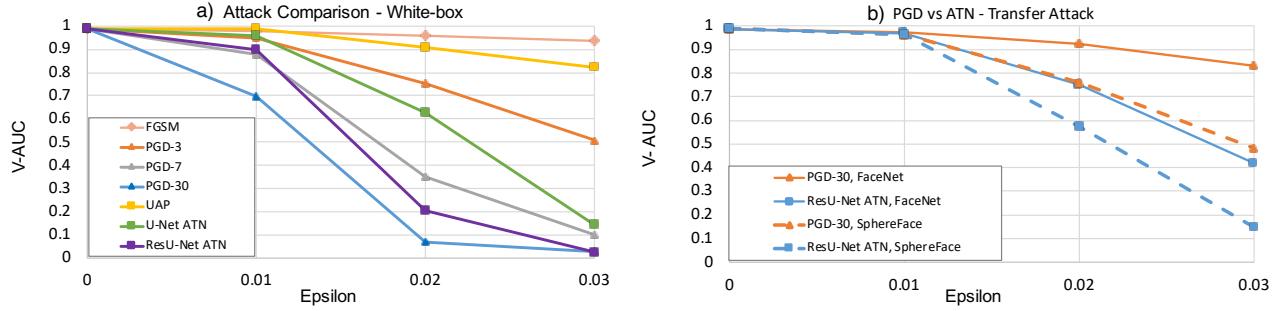


Fig. 5. Comparison of PGD and ATN based attacks. (a) compares white-box attacks on the single RN-SF-1 model. (b) compares transfer attacks optimized on the six RN-SF-6 models and evaluated on two different models.



Fig. 6. Sample adversarial images generated at $\epsilon = 0.03$ and their benign counterparts. Photo credit: Georges Biard, Christopher Michel, honeyfitz

from the test set. For a fair comparison, we drop the L_{pips} term from the loss and train purely to maximize the cosine distance with an L_∞ constraint. Figure 5a shows white-box attack success rate of PGD and ATN attacks on the RN-SF-1 model. As discussed in Section 3.4, Residual U-Net ATN architecture provides a large improvement over a basic U-net and bridges the white-box performance gap between the ATN and PGD-30.

We also performed an ensemble attack on the six models from RN-SF-6. Running PGD-30 against six surrogate models simultaneously took more than three seconds per image, while the ATN’s forward pass was the same complexity as other experiments - more than $10,000 \times$ faster than PGD-30. Table 3 reports the timing comparison of ATN and PGD attacks. In addition to being fast, ATNs learn attacks that generalize effectively to new models. We evaluated how well the perturbed images transferred to two different models. First, we evaluated against a ResNet+SphereFace model that is similar to the RN-SF-6 models, but has a different number of layers. Second, we evaluated against an open source model from the FaceNet repository⁶. This model uses a different architecture (Inception ResNet), loss (DeepID) and training procedure. We did not do any parameter tuning based on this model, so it serves as an independent validation of the transferability of our attacks.

Figure 5b compares the attacks at different L_∞ thresholds. As expected, transferring an attack from RN-SF-6 to the FaceNet model was more difficult than the ResNet+SphereFace model. However, in both cases the ATN attack is effective at $\epsilon = 0.02$ and transfers much better than PGD to the new models.

5.3 UAP vs ATN

We find that attacks utilizing ATNs outperform the UAP attacks at the same level of perturbation. Since the goal of finding a single input-agnostic perturbation is more challenging than finding one perturbation per image, a higher amount of distortion is required for a successful attack using UAPs as compared to the ATN based attacks. This is indicated by less successful attack metrics (higher V-AUC) from UAPs in Figure 5a. However, it is important to note that UAPs pose a significant threat to face recognition models since they can be easily shared amongst attackers and are simpler to implement as compared to ATNs.

⁶ <https://github.com/davidsandberg/facenet>

Process	Avg Wall-Clock Time (seconds)	
	GPU	CPU
RN-SF-1	2.93e-2	1.02e-1
ATN	2.83e-3	5.67e-2
UAP	1.89e-4	5.39e-3
PGD	3.73	365.2

Table 3. Average Wall-Clock time in seconds required for generating a single adversarial image on GPU and CPU platforms using different attacks. Time for RN-SF-1 process indicates the forward pass computation time for a single ResNet Face Recognition model.

5.4 Attacking Public APIs

We demonstrate the effectiveness of our attacks against commercial face recognition systems. These systems are black-box, proprietary, and are abstracted away through a web-based API. We evaluate our perturbations against the Amazon (AWS) Rekognition and Microsoft Azure Face services.

Face Verification: In this setting, we target the *CompareFaces* API in AWS and the *verify_face_to_face* API in the Azure Face client. We prepare a total of 1000 image pairs (500 positive and 500 negative) and report the verification metrics in Table 4.

Face Identification: We target the *SearchFaces* API in AWS Rekognition. The API accepts a gallery of N faces $x_1, x_2, x_3 \dots x_N$ and a query image x_q , and returns similar faces to the query image from those in the gallery, ranked in order of similarity to the query image. We generate a gallery of 500 benign faces each with unique identities and 500 adversarial samples by adversarially perturbing alternate images of the same identities as those in the gallery, resulting in a total of 500 trials. We report the Rank-1 accuracy of this experiment in Table 4.

Input type	Verification		Identification		AWS
	V-Acc. (%)	Recall (%)	AWS	Azure	
Clean images	95.5	91.0	91.0	83.0	82.0
Ensemble ATN	64.7	50.1	30.2	2.1	16.4

Table 4. ATN attack results at $\epsilon = 0.03$ against AWS and Azure face recognition APIs. The ATN was trained jointly on RN-SF-6 and IN-SF-4. Recall(%) indicates the verification accuracy on only the positive pairs in the evaluation set. For verification, we use the default match threshold 0.5 for both AWS and Azure.

6 Conclusion

We develop real-time attacks using ATNs for fooling face recognition systems. Using our ResU-Net ATN model, we bridge the performance gap between ATN and gradient-based PGD attacks while being several orders of magnitude faster than PGD attacks. We demonstrate that adversarial examples generated using ATNs can effectively bypass face recognition systems in both white-box and black-box transfer attack settings. Adversarial examples generated from our framework can bypass commercial face recognition APIs in a complete black-box setting and reduce face identification accuracy from 82% to 16.4%.

Acknowledgements

This research was funded under Defense Advanced Research Projects Agency contract HR00112090093. This research was, in part, funded by the U.S. Government. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Government. Approved for Public Release, Distribution Unlimited.

References

1. Fawkes press release, <https://sandlab.cs.uchicago.edu/fawkes/#press>
2. The new york times, <https://www.nytimes.com/2020/08/03/technology/fawkes-tool-protects-photos-from-facial-recognition.html>
3. Abdelhafiz, D., Nabavi, S., Ammar, R., Yang, C., Bi, J.: Residual deep learning system for mass segmentation and classification in mammography. In: Proceedings of the 10th ACM International Conference on Bioinformatics, Computational Biology and Health Informatics (2019)
4. Athalye, A., Carlini, N., Wagner, D.: Obfuscated gradients give a false sense of security: Circumventing defenses to adversarial examples. In: Proceedings of the 35th International Conference on Machine Learning, ICML 2018 (2018)
5. Baluja, S., Fischer, I.: Learning to attack: Adversarial transformation networks. In: Proceedings of AAAI (2018)
6. Biggio, B., Corona, I., Maiorca, D., Nelson, B., Šrndić, N., Laskov, P., Giacinto, G., Roli, F.: Evasion attacks against machine learning at test time. In: Blockeel, H., Kersting, K., Nijssen, S., Železný, F. (eds.) Machine Learning and Knowledge Discovery in Databases (2013)
7. Byun, J., Go, H., Kim, C.: Geometrically adaptive dictionary attack on face recognition. In: Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision (2022)
8. Cao, Q., Shen, L., Xie, W., Parkhi, O., Zisserman, A.: Vggface2: A dataset for recognising faces across pose and age. 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018) (2018)
9. Carlini, N., Wagner, D.A.: Towards evaluating the robustness of neural networks. 2017 IEEE Symposium on Security and Privacy (SP) (2017)
10. Chandrasekaran, V., Gao, C., Tang, B., Fawaz, K., Jha, S., Banerjee, S.: Face-off: Adversarial face obfuscation. Proceedings on Privacy Enhancing Technologies (2021)
11. Cherepanova, V., Goldblum, M., Foley, H., Duan, S., Dickerson, J.P., Taylor, G., Goldstein, T.: Lowkey: Leveraging adversarial attacks to protect social media users from facial recognition. In: International Conference on Learning Representations (2021), <https://openreview.net/forum?id=hJmtwocEqzc>
12. Dong, Y., Su, H., Wu, B., Li, Z., Liu, W., Zhang, T., Zhu, J.: Efficient decision-based black-box adversarial attacks on face recognition. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (2019)
13. Goodfellow, I.J., Shlens, J., Szegedy, C.: Explaining and harnessing adversarial examples. stat **1050**, 20 (2015)
14. He, K., Zhang, X., Ren, S., Sun, J.: Identity mappings in deep residual networks. ArXiv **abs/1603.05027** (2016)
15. Hussain, S., Neekhara, P., Dolhansky, B., Bitton, J., Canton Ferrer, C., McAuley, J., Koushanfar, F.: Exposing vulnerabilities of deepfake detection systems with robust attacks. ACM Journal of Digital Threats: Research and Practice (2022). <https://doi.org/10.1145/3464307>
16. Hussain, S., Neekhara, P., Jere, M., Koushanfar, F., McAuley, J.: Adversarial deepfakes: Evaluating vulnerability of deepfake detectors to adversarial examples. In: WACV (2021)
17. Isola, P., Zhu, J.Y., Zhou, T., Efros, A.A.: Image-to-image translation with conditional adversarial networks. CVPR (2017)
18. Kandel, M.E., He, Y.R., Lee, Y.J., Chen, T.H.Y., Sullivan, K.M., Aydin, O., Saif, M.T.A., Kong, H., Sobh, N., Popescu, G.: Phase imaging with computational specificity (pics) for measuring dry mass changes in sub-cellular compartments. Nature communications (2020)
19. Kingma, D.P., Ba, J.: Adam: A method for stochastic optimization. CoRR **abs/1412.6980** (2015)
20. Kurakin, A., Goodfellow, I.J., Bengio, S.: Adversarial machine learning at scale. In: 5th International Conference on Learning Representations, ICLR (2017)
21. Li, H., Chen, D., Nailon, B., Davies, M.E., Laurenson, D.: Improved breast mass segmentation in mammograms with conditional residual u-net. ArXiv **abs/1808.08885** (2018)
22. Liu, W., Wen, Y., Yu, Z., Li, M., Raj, B., Song, L.: Spherenet: Deep hypersphere embedding for face recognition. 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) pp. 6738–6746 (2017)
23. Madry, A., Makelov, A., Schmidt, L., Tsipras, D., Vladu, A.: Towards deep learning models resistant to adversarial attacks. In: International Conference on Learning Representations (2018)

24. Moosavi-Dezfooli, S., Fawzi, A., Fawzi, O., Frossard, P.: Universal adversarial perturbations. In: 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR) (2017)
25. Papernot, N., McDaniel, P., Jha, S., Fredrikson, M., Celik, Z.B., Swami, A.: The limitations of deep learning in adversarial settings. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P) (2016)
26. Papernot, N., McDaniel, P.D., Goodfellow, I.J.: Transferability in machine learning: from phenomena to black-box attacks using adversarial samples. CoRR **abs/1605.07277** (2016), <http://arxiv.org/abs/1605.07277>
27. Pinkus, A.: Approximation theory of the mlp model in neural networks. *Acta Numerica* **8**, 143 – 195 (1999)
28. Rajabi, A., Bobba, R.B., Rosulek, M., Wright, C.V., Feng, W.c.: On the (im) practicality of adversarial perturbation for image privacy. Proceedings on Privacy Enhancing Technologies pp. 85–106 (2021)
29. Ronneberger, O., Fischer, P., Brox, T.: U-net: Convolutional networks for biomedical image segmentation. In: Medical Image Computing and Computer-Assisted Intervention – MICCAI. Springer International Publishing (2015)
30. Rozsa, A., Günther, M., Boult, T.E.: Lots about attacking deep features. In: 2017 IEEE International Joint Conference on Biometrics (IJCB). pp. 168–176 (2017). <https://doi.org/10.1109/BTAS.2017.8272695>
31. Shan, S., Wenger, E., Zhang, J., Li, H., Zheng, H., Zhao, B.Y.: Fawkes: Protecting privacy against unauthorized deep learning models. In: 29th USENIX Security Symposium (2020)
32. Shi, Y., Wang, S., Han, Y.: Curls & whey: Boosting black-box adversarial attacks. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2019)
33. Sun, Y., Wang, X., Tang, X.: Deep learning face representation from predicting 10,000 classes. 2014 IEEE Conference on Computer Vision and Pattern Recognition (2014)
34. Szegedy, C., Ioffe, S., Vanhoucke, V., Alemi, A.A.: Inception-v4, inception-resnet and the impact of residual connections on learning. In: AAAI (2017)
35. Szegedy, C., Zaremba, W., Sutskever, I., Bruna, J., Erhan, D., Goodfellow, I.J., Fergus, R.: Intriguing properties of neural networks. CoRR **abs/1312.6199** (2013), <http://arxiv.org/abs/1312.6199>
36. Zhang, R., Isola, P., Efros, A.A., Shechtman, E., Wang, O.: The unreasonable effectiveness of deep features as a perceptual metric. In: CVPR (2018)