A FRANK-WOLFE FRAMEWORK FOR EFFICIENT AND EFFECTIVE ADVERSARIAL ATTACKS

Anonymous authors
Paper under double-blind review

ABSTRACT

Depending on how much information an adversary can access to, adversarial attacks can be classified as white-box attack and black-box attack. In both cases, optimization-based attack algorithms can achieve relatively low distortions and high attack success rates. However, they usually suffer from poor time and query complexities, thereby limiting their practical usefulness. In this work, we focus on the problem of developing efficient and effective optimization-based adversarial attack algorithms. In particular, we propose a novel adversarial attack framework for both white-box and black-box settings based on the non-convex Frank-Wolfe algorithm. We show in theory that the proposed attack algorithms are efficient with an $O(1/\sqrt{T})$ convergence rate, which, to our knowledge, is the first convergence rate analysis for the zeroth-order non-convex Frank-Wolfe type algorithm. The empirical results on attacking Inception V3 model with the ImageNet dataset also verify the efficiency and effectiveness of the proposed algorithms. They attain a 100% attack success rate in both white-box and black-box attacks, and are more time and query efficient than the state-of-the-art baseline algorithms.

1 INTRODUCTION

Deep Neural Networks (DNNs) have made many breakthroughs in different areas of artificial intelligence such as image classification (Krizhevsky et al., 2012; He et al., 2016), object detection (Ren et al., 2015; Girshick, 2015), and speech recognition (Mohamed et al., 2012; Bahdanau et al., 2016). However, recent studies show that deep neural networks can be vulnerable to adversarial examples (Szegedy et al., 2013; Goodfellow et al., 2015) – a tiny perturbation on an image that is almost invisible to human eyes could mislead a well-trained image classifier towards misclassification. Soon later this is proved to be not a coincidence: similar phenomena have been observed in other problems such as speech recognition (Carlini et al., 2016), visual QA (Xu et al., 2017), image captioning (Chen et al., 2017a), machine translation (Cheng et al., 2018b), reinforcement learning (Pattanaik et al., 2018), and even on systems that operate in the physical world (Kurakin et al., 2016).

Depending on how much information an adversary can access to, adversarial attacks can be classified into two classes: white-box attack (Szegedy et al., 2013; Goodfellow et al., 2015) and black-box attack (Papernot et al., 2016a; Chen et al., 2017c). In the white-box setting, the adversary has full access to the target model, while in the black-box setting, the adversary can only access the input and output of the target model but not its internal configurations. Among the approaches proposed for white-box and black-box attacks, optimization-based methods (Carlini & Wagner, 2017; Chen et al., 2017b; Ilyas et al., 2018; Cheng et al., 2018a) are the most effective: they usually achieve relatively low distortions and high attack success rates. However, these methods are not that efficient. In the white-box setting, they need to solve constrained optimization problems (Carlini & Wagner, 2017), and are usually significantly slower than the gradient-based methods such as Fast Gradient Sign Method (FGSM) (Goodfellow et al., 2015) or Iterative FGSM (I-FGM) (Kurakin et al., 2016). In the black-box setting, it becomes even more severe since they need to make coordinate-wise gradient estimations (Chen et al., 2017c). Therefore, a large number of queries are needed for them to perform a successful attack, especially when the data dimension is large. For example, attacking a $299 \times 299 \times 3$ Imagenet image may take them hundreds of thousands of queries. This significantly limits their practical usefulness since they can be easily defeated by limiting the number of queries that an adversary can make to the target model.

In this study, we aim to examine the following questions in this study:
Can we improve the efficiency of the optimization-based attack algorithms? In other words, can we use less time and queries to conduct adversarial attacks?

In this work, we provide an affirmative answer to this question by proposing an efficient Frank-Wolfe optimization framework for both white-box and black-box attacks. In summary, we make the following main contributions:

- We propose a novel Frank-Wolfe based adversarial attack framework. The white-box attack algorithm is an iterative first-order method which admits the fast gradient sign method (FGSM) as the one-step special case. And the corresponding black-box attack algorithm adopts zeroth-order optimization with two sensing vector options (either from the Euclidean unit sphere or from the standard Gaussian distribution) provided.
- We show that the proposed white-box and black-box attack algorithms enjoy an $O(1/\sqrt{T})$ convergence rate. To the best of our knowledge, we provide the first convergence rate analysis for the zeroth-order non-convex Frank-Wolfe type algorithm.
- We show that the query complexity of the proposed black-box attack algorithm is linear in data dimension $d$.
- Our empirical results on attacking Inception V3 model with the ImageNet dataset show that (i) the proposed white-box attack algorithm is more efficient than all the baseline white-box algorithms evaluated here, and (ii) the proposed black-box attack algorithm is highly efficient and is also the only one algorithm that achieves a 100% attack success rate.

2 RELATED WORK

There is a large body of work on adversarial attacks. In this section, we review the most relevant work in both white-box and black-box attack settings, as well as the non-convex Frank-Wolfe optimization.

White-box Attacks: Szegedy et al. (2013) proposed to use box-constrained L-BFGS algorithm for conducting white-box attacks. Goodfellow et al. (2015) proposed the Fast Gradient Sign Method (FGSM) based on linearization of the network as a simple alternative to L-BFGS. Kurakin et al. (2016) proposed to iteratively perform one-step FGSM (Goodfellow et al., 2015) algorithm and clips the adversarial point back to the distortion limit after every iteration. It is called Basic Iterative Method (BIM) or I-FGM in the literature. Madry et al. (2018) showed that for the $L_\infty$ norm case, BIM/I-FGM is equivalent to Projected Gradient Descent (PGD), which is a standard tool for constraint optimization. Papernot et al. (2016b) proposed JSMA to greedily attack the most significant pixel based on the Jacobian-based saliency map. Moosavi-Dezfooli et al. (2016) proposed attack methods by projecting the data to the closest separating hyperplane. Carlini & Wagner (2017) introduced the so-called CW attack by proposing multiple new loss functions for generating adversarial examples. Chen et al. (2017b) followed CW’s framework and use an Elastic Net term as the distortion penalty.

Black-box Attacks: One popular family of black-box attacks (Hu & Tan, 2017; Papernot et al., 2016a, 2017) is based on the transferability of adversarial examples (Liu et al., 2018; Bhagoji et al., 2017), where an adversarial example generated for one DNN may be reused to attack other neural networks. This allows the adversary to construct a substitute model that mimics the targeted DNN, and then attack the constructed substitute model using white-box attack methods. However, this type of attack algorithms usually suffer from large distortions and relatively low success rates (Chen et al., 2017c). To address this issue, Chen et al. (2017c) proposed the Zeroth-Order Optimization (ZOO) algorithm that extends the CW attack to the black-box setting and uses a zeroth-order optimization approach to conduct the attack. Although ZOO achieves much higher attack success rates than the substitute model-based black-box attacks, it suffers from a poor query complexity since its naive implementation requires to estimate the gradients of all the coordinates (pixels) of the image. To improve its query complexity, several approaches have been proposed. For example, Tu et al. (2018) introduces an adaptive random gradient estimation algorithm and a well-trained Autoencoder to speed up the attack process. Ilyas et al. (2018) and Liu et al. (2018) improved ZOO’s query complexity by using Natural Evolutionary Strategies (NES) (Wierstra et al., 2014; Salimans et al., 2017) and active learning, respectively.

Non-convex Frank-Wolfe Algorithms: The Frank-Wolfe algorithm (Frank & Wolfe, 1956), also known as the conditional gradient method, is an iterative optimization method for constrained op-
According to the attack purposes, attacks can be divided into two categories: untargeted attack and targeted attack. Denote $P$ by $\|p\|$. Let us define $f$ can be extended to untargeted attack straightforwardly. Focus on the strictly harder targeted attack setting. It is worth noting that our proposed algorithm uses Frank-Wolfe for distributionally robust training (Sinha et al., 2018).

3 METHODOLOGY

3.1 Notations

Throughout the paper, scalars are denoted by lower case letters, vectors by lower case bold face letters and sets by calligraphy upper case letters. For a vector $x \in \mathbb{R}^d$, we denote the $L_p$ norm of $x$ by $\|x\|_p = (\sum_{i=1}^d |x_i|^p)^{1/p}$. Specially, for $p = \infty$, the $L_{\infty}$ norm of $x$ by $\|x\|_\infty = \max_{i=1}^d |x_i|$. We denote $P_X(x)$ as the projection operation of projecting vector $x$ into the set $X$.

3.2 Problem Formulation

According to the attack purposes, attacks can be divided into two categories: untargeted attack and targeted attack. In particular, untargeted attack aims to turn the prediction into any incorrect label, while the targeted attack, which is considerably harder, requires to mislead the classifier to a specific target class. In this work, we follow the literature (Carlini & Wagner, 2017; Ilyas et al., 2018) and focus on the strictly harder targeted attack setting. It is worth noting that our proposed algorithm can be extended to untargeted attack straightforwardly.

Let us define $f(\cdot)$ as the classification loss function of the targeted DNN. For targeted attacks, we aim to learn an adversarial example $x$ that is close enough to the original input $x_{ori}$ and can be misclassified to the target class $y_{tar}$. The corresponding optimization problem is defined as:

\[
\min_x \quad f(x, y_{tar}) \\
\text{subject to} \quad \|x - x_{ori}\|_p \leq \epsilon. \tag{3.1}
\]

Evidently, the constraint set $X := \{x \mid \|x - x_{ori}\|_p \leq \epsilon\}$ is a bounded convex set when $p \geq 1$. Normally, $p = 2$ and $p = \infty$ are used to measure the distortions $\|x - x_{ori}\|_p$, resulting in $L_2$ attack model and $L_\infty$ attack model respectively. In this work, we study both models.

3.3 Frank-Wolfe White-box Attacks

Frank-Wolfe algorithm (Frank & Wolfe, 1956), also known as the conditional gradient descent, is a popular optimization tool for constraint optimization. Different from PGD that first performs gradient descent followed by a projection step at each iteration, Frank-Wolfe algorithm calls a Linear Minimization Oracle (LMO) over the the constraint set $X$ at each iteration, i.e.,

\[\text{LMO} = \arg\min_{v \in X} \langle v, \nabla f(x_t, y_{tar}) \rangle.\]

The LMO can be seen as the minimization of the first-order Taylor expansion of $f(\cdot)$ at point $x_t$:

\[\min_{v \in X} f(x_t) + \langle v - x_t, \nabla f(x_t, y_{tar}) \rangle.\]

By calling LMO, Frank Wolfe solves the linear problem in $X$ and then perform weighted average with previous iterate to obtain the final update formula.

We present our proposed Frank-Wolfe white-box attack algorithm in Algorithm 1, which is built upon the original Frank-Wolfe algorithm. The key difference between Algorithm 1 and the standard Frank-Wolfe algorithm is in Line 3 where the LMO is called over a slightly relaxed constraint set $X' := \{x \mid \|x - x_{ori}\|_p \leq \lambda \epsilon\}$ with $\lambda \geq 1$, instead of the original constraint set $X$. When $\lambda = 1$, set $X'$ reduces to $X$, and Algorithm 1 reduces to standard Frank Wolfe. We argue that this modification makes our algorithm more general, and gives rise to better attack results.

The LMO solution itself can be expensive to obtain in general. Fortunately, applying Frank-Wolfe to solve (3.1) actually gives us a close-form LMO solution. We provide the solutions of LMO (Line 3.2 P

Under review as a conference paper at ICLR 2019

3
Algorithm 1 Frank-Wolfe White-box Attack Algorithm

1: input: number of iterations $T$, step sizes $\{\gamma_t\}$, $\lambda > 0$, original image $x_{ori}$, target label $y_{tar}$;
2: $x_0 = x_{ori}$
3: for $t = 0, \ldots, T - 1$ do
4: $v_t = \arg\min_{v \in \mathcal{X}} \langle v, \nabla f(x_t, y_{tar}) \rangle$ // LMO
5: $d_t = v_t - x_t$
6: $x_{t+1} = x_t + \gamma_t d_t$
7: if $\lambda > 1$ then
8: $x_{t+1} = \mathcal{P}_X(x_{t+1})$
9: end if
10: end for
11: output: $x_T$

\[ v = \frac{\lambda \epsilon \cdot \nabla f(x_t, y_{tar})}{\|\nabla f(x_t, y_{tar})\|_2} + x_{ori}, \quad (L_2 \text{ norm}) \]
\[ v = -\lambda \epsilon \cdot \text{sign}(\nabla f(x_t, y_{tar})) + x_{ori}, \quad (L_\infty \text{ norm}) \]

The derivation can be found in the supplemental materials.

Note that when $T = 1$, $\lambda = 1$, substituting the above LMO solutions into Algorithm 1 yields the final update of $x_1 = x_0 - \gamma_t \epsilon \cdot \nabla f(x_t, y_{tar})$, which reduces to FGSM when $\gamma_t = 1$. Similar derivation also applies to $L_2$ norm case. Therefore, just like PGD, our proposed Frank-Wolfe white-box attack also includes FGSM (FGM) as a one-step special instance.

3.4 Frank-Wolfe Black-box Attacks

Next we consider the black-box setting, where we cannot perform back-propagation to calculate the gradient of the loss function anymore. Instead, we can only query the DNN system’s outputs with specific inputs. To clarify, here the output refers to the logit layer’s output (confidence scores for classification), not the final prediction label. The label-only setting is doable under our framework, but will incur extra difficulty such as designing new loss functions. For simplicity, here we consider the confidence score output.

We propose a zeroth-order Frank-Wolfe based algorithm to solve this problem. Algorithm 2 show our proposed Frank-Wolfe black-box attack algorithm. The key difference between our proposed black-box attack and white-box attack is one extra gradient estimation step, which is presented in Line 4 in Algorithm 1. Also note that for the final output, we provide two options. While option II is the common choice in practice, option I is also provided for the ease of theoretical analysis.

Algorithm 2 Frank-Wolfe Black-box Attack Algorithm

1: input: number of iterations $T$, step sizes $\{\gamma_t\}$, $\lambda > 0$, original image $x_{ori}$, target label $y_{tar}$;
2: $x_0 = x_{ori}$
3: for $t = 0, \ldots, T - 1$ do
4: $q_t = \text{ZERO_ORD_GRAD}_{\text{EST}}(x_t, y_{tar})$ // Algorithm 3
5: $v_t = \arg\min_{v \in \mathcal{X}} \langle v, q_t \rangle$
6: $d_t = v_t - x_t$
7: $x_{t+1} = x_t + \gamma_t d_t$
8: if $\lambda > 1$ then
9: $x_{t+1} = \mathcal{P}_X(x_{t+1})$
10: end if
11: end for
12: Option I: $x_a$ is uniformly random chosen from $\{x_t\}_{t=1}^T$
13: Option II: $x_a = x_T$
14: output: $x_a$

The extra clipping operation in FGSM is to project to the additional box constraint for image classification task. We will also need this clipping operation at the end of each iteration for specific tasks such as image classification.
As many other zeroth-order optimization algorithms (Shamir [2017]; Flaxman et al. [2005]), Algorithm 3 uses symmetric finite differences to estimate the gradient and therefore, gets rid of the dependence on back-propagation in white-box setting. Different from Chen et al. (2017c), here we do not utilize natural basis as our sensing vectors, instead, we provide two options: one is to use vectors uniformly sampled from Euclidean unit sphere and the other is to use vectors uniformly sampled from standard multivariate Gaussian distribution. This will greatly improve the gradient estimation efficiency comparing to sensing with natural basis as such option will only be able to estimate one coordinate of the gradient vector per query. In practice, both options here provide us competitive experimental results. It is worth noting that NES method (Wierstra et al., 2014) with antithetic sampling (Salimans et al., 2017) used in Ilyas et al. (2018) yields similar formula as our Option II in Algorithm 3.

Algorithm 3 Zeroth-Order Gradient Estimation (ZERO_ORD_GRAD_EST)

1: parameters: number of gradient estimation samples $b$, sampling parameter $\delta_i$;
2: $q = 0$
3: for $i = 1, \ldots, b$ do
4:  Option I: Sample $u_i$ uniformly from the Euclidean unit sphere with $\|u_i\|^2_2 = 1$, $\lambda = d$
5:  Option II: Sample $u_i$ uniformly from the standard Gaussian distribution $\mathcal{N}(0, I)$, $\lambda = 1$
6:  $q = q + \frac{1}{\lambda d^2}(f(x_t + \delta_i u_i, y_{\text{tar}}) - f(x_t - \delta_i u_i, y_{\text{tar}}))u_i$
7: end for
8: output: q

4 MAIN THEORY

In this section, we establish the convergence guarantees for our proposed Frank-Wolfe adversarial attack algorithms described in Section 3. First, we introduce the convergence criterion for our Frank-Wolfe adversarial attack framework.

4.1 CONVERGENCE CRITERION

The loss function for common DNN models are generally nonconvex. In addition, (3.1) is a constrained optimization. For such general nonconvex constrained optimization, we typically adopt the Frank-Wolfe gap as the convergence criterion (since gradient norm of $f$ is no longer a proper criterion for constrained optimization problems): 

$$g(x_t) = \max_{x \in \mathcal{X}} \langle x - x_t, -\nabla f(x_t, y_{\text{tar}}) \rangle.$$ 

Note that for the Frank-Wolfe gap, we always have $g(x_t) \geq 0$ and $x_t$ is a stationary point for the constrained optimization problem if and only if $g(x_t) = 0$. Also the Frank-Wolfe gap is affine invariant and do not tie to any specific choice of norm, which makes itself a perfect convergence criterion for Frank-Wolfe based algorithms.

4.2 CONVERGENCE GUARANTEE FOR FRANK-WOLFE WHITE-BOX ATTACK

Before we are going to provide the convergence guarantee of Frank-Wolfe white-box attack (Algorithm 1), we introduce the following assumptions that are essential to the convergence analysis.

Assumption 4.1. Function $f(\cdot)$ is $L$-smooth with respect to $x$, i.e., for any $x, x'$, it holds that

$$f(x', y) \leq f(x, y) + \nabla f(x, y)'(x' - x) + \frac{L}{2}\|x' - x\|^2_2.$$ 

Assumption 4.1 is a standard assumption in nonconvex optimization, and is also adopted in other Frank-Wolfe literature such as Lacoste-Julien (2016); Reddi et al. (2016). Note that even though the smoothness assumption does not hold for general DNN models, a recent study (Santurkar et al., 2018) shows that batch normalization that is used in many modern DNNs such as Inception V3 model, actually makes the optimization landscape significantly smoother.

Footnote: The original argument in Santurkar et al. (2018) refers to the smoothness with respect to each layer’s parameters. Note that the first layer’s parameters are in the mirror position (in terms of backpropagation) as the network inputs. Therefore, the argument in Santurkar et al. (2018) can also be applied here with respect to the network inputs.
**Assumption 4.1.** Set $\mathcal{X}$ is bounded with diameter $D$, i.e., $\|x - x'\|_2 \leq D$ for all $x, x' \in \mathcal{X}$.

Assumption 4.2 implies that the input space is bounded. For common tasks such as image classification, given the fact that images have bounded pixel range and $\epsilon$ is a small constant, this assumption trivially holds.

Now we present the theorem, which characterizes the convergence rate of our proposed Frank-Wolfe white-box adversarial attack algorithm presented in Algorithm 1.

**Theorem 4.3.** Under Assumptions 4.1 and 4.2, let $\gamma = \sqrt{2(f(x_0, y) - f(x^*, y))/(LD^2T)}$, denote $g_T = \min_{1 \leq k \leq T} g(x_k)$ where $\{x_k\}_{k=1}^T$ are iterates in Algorithm 1 with $\lambda = 1$, we have:

$$ \tilde{g}_T \leq \sqrt{\frac{LD^2(f(x_0, y) - f(x^*, y))}{2T}}, $$

where $x^*$ is the optimal solution to (3.1).

**Remark 4.4.** Theorem 4.3 suggests that our proposed Frank-Wolfe white-box attack algorithm achieves an $O(1/\sqrt{T})$ rate of convergence.

### 4.3 CONVERGENCE GUARANTEE FOR FRANK-WOLFE BLACK-BOX ATTACK

Next we analyze the convergence of our proposed Frank-Wolfe black-box adversarial attack algorithm presented in Algorithm 2.

In order to prove the convergence of our proposed Frank-Wolfe black-box attack algorithm, we need the following additional assumption that $\|\nabla f(0, y)\|_2$ is bounded.

**Assumption 4.5.** Gradient of $f(\cdot)$ at zero point $\nabla f(0, y)$ satisfies $\max_y \|\nabla f(0, y)\|_2 \leq C_g$.

Following the analysis in Shamir (2017), let $f_\delta(x, y) = \mathbb{E}_u[f(x + \delta u, y)]$, which is the smoothed version of $f(x, y)$. This smoothed function value plays a central role in our theoretical analysis, since it bridges the finite difference gradient approximation with the actual gradient. The following lemma shows this relationship.

**Lemma 4.6.** For the gradient estimator $q_\epsilon$ in Algorithm 3, its expectation and variance satisfy

$$ \mathbb{E}[q_\epsilon] = \nabla f_\delta(x_t, y_{tar}), \quad \mathbb{E}\|q_\epsilon - \mathbb{E}[q_\epsilon]\|^2_2 \leq \frac{1}{b} \left(2d(C_g + LD)^2 + \frac{1}{2} \delta^2 L^2 d^2 \right). $$

Now we are going to present the theorem, which characterizes the convergence rate of Algorithm 2.

**Theorem 4.7.** Under Assumptions 4.1, 4.2 and 4.5, let $\gamma = \sqrt{2(f(x_0, y) - f(x^*, y))/(LD^2T)}$, $b = Td$ and $\delta_e = \sqrt{2/Td^2}$, suppose we use Option I in Algorithm 2 and option II for Algorithm 3, then the output $x_a$ from Algorithm 2 with $\lambda = 1$ satisfies:

$$ g(x_a) \leq \frac{D}{\sqrt{2T}} \left(\sqrt{L(f(x_0, y) - f(x^*, y))} + 2(L + C_g + LD)\right), $$

where $x^*$ is the optimal solution to (3.1).

**Remark 4.8.** Theorem 4.7 suggests that Algorithm 2 also enjoys an $O(1/\sqrt{T})$ rate of convergence. In terms of query complexity, the total number of queries needed is $Tb = T^2 d$, which is linear in the data dimension $d$. In fact, in the experiment part, we observed that this number can be substantially smaller than $d$, e.g., $b = 25$, which is much lower than the theorem suggests. Note that although we only prove for option II in Algorithm 3, our result can be readily extended to Option I (the Gaussian sensing vector case).

### 5 EXPERIMENTS

In this section, we present the experimental results for our proposed Frank-Wolfe attack framework against other state-of-the-art adversarial attack algorithms in both white-box and black-box settings. All of our experiments are conducted on Amazon AWS p3.2xlarge servers which come with Intel Xeon E5 CPU and one NVIDIA Tesla V100 GPU (16G RAM). All experiments are implemented in Tensorflow platform version 1.10.0 within Python 3.6.4.
Table 1: Comparison of $L_2$ norm based white-box attacks on Inception V3 model with $\epsilon = 5$. We report attack success rate, average time and average distortion.

<table>
<thead>
<tr>
<th>METHODS</th>
<th>SUCCESS RATE (%)</th>
<th>AVERAGE TIME (s)</th>
<th>AVERAGE DISTORTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FGM</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>BIM/ I-FGM</td>
<td>100</td>
<td>197.67</td>
<td>0.79</td>
</tr>
<tr>
<td>CW</td>
<td>100</td>
<td>167.07</td>
<td><strong>0.55</strong></td>
</tr>
<tr>
<td>EAD</td>
<td>100</td>
<td>175.20</td>
<td>1.07</td>
</tr>
<tr>
<td>FW-White</td>
<td>100</td>
<td><strong>28.39</strong></td>
<td>0.87</td>
</tr>
</tbody>
</table>

5.1 Evaluation Setup and Metrics

We test the attack effectiveness of all algorithms by evaluating on a pre-trained Inception V3 model (Szegedy et al., 2016) that is trained on ImageNet dataset (Deng et al., 2009). The pre-trained model is reported to have a 78% top-1 accuracy. We randomly choose 200 images from the ImageNet validation set that are verified to be correctly classified by the pre-trained model and also randomly choose a target class for each image. Each image has a dimension of $299 \times 299 \times 3$ and we test all attack algorithms through the same randomly chosen data samples and target labels.

We test for both $L_2$ norm based and $L_\infty$ norm based attacks. For $L_2$ norm based attack, we set $\epsilon = 5$ and for $L_\infty$ based attack, we set $\epsilon = 0.05$. For white-box attack, we restrict a maximum of 1,000 iterations per attack for each method. And for black-box attack, we set a maximum query limit of 500,000 per attack per image for each method.

For all algorithms, we stop the algorithm when a successful attack is found. For our proposed black-box attack, we use option II in Algorithm 2 and test both options in Algorithm 3. We set the number of gradient estimation samples $b = 25$ for Algorithm 2. More detailed description on parameter settings can be found in the supplemental materials.

We evaluate the final performance through attack success rate where the success is defined as making the classifier output the exact target class label (not any incorrect labels). We also measure average attack time per image, average distortion (only on successful attacked samples) and average number of queries needed (only for black-box attack) per image. For a fair time comparison, even though some of the algorithms including ours can be written in batch form (attack multiple images at one time), all algorithms are set to attack one image at a time.

5.2 Baseline Methods

We compare the proposed algorithms with several state-of-the-art baseline algorithms. Specifically, we compare the proposed white-box attack algorithm with (i) FGM (FGSM) (Goodfellow et al., 2015) (ii) BIM / I-FGM (Kurakin et al., 2016) (iii) CW attack (Carlini & Wagner, 2017) and (iv) EAD attack (Chen et al., 2017b). We compare the proposed black-box attack algorithm with (i) ZOO attack (Chen et al., 2017c) and (ii) NES-PGD attack (Ilyas et al., 2018).

5.3 White-box Attack Experiments

In this subsection, we present the white-box attack experiments on Inception V3 model. Tables 1 and 2 present our experimental results for $L_2$ norm and $L_\infty$ norm based white-box attacks respectively. As we can observe from the tables, the attack success rate is basically 100% for every method except for the simplest FGM (FGSM) attack. For the other baselines in the $L_2$ norm case, CW method achieves the smallest average distortion, yet it comes with an expansive time cost. EAD method does not have either time advantage or distortion advantage in this experiment, probably due to its different motivation in attacking. BIM/ I-FGM has relatively small average distortion, yet it also costs the most attack time among all methods. On the other hand, our proposed algorithm achieves the shortest attack time with moderate distortion. It significantly reduces the time complexity needed for attacking data with large dimensionality. For the $L_\infty$ norm case, CW method takes significantly longer time and does not perform very well on average distortion either. This is largely due to the special design of CW method to make it possible for $L_\infty$ norm attack. Again, our proposed white-box attack algorithm achieves the shortest average attack time and a moderate average distortion.
Table 2: Comparison of $L_\infty$ norm based white-box attacks on Inception V3 model with $\epsilon = 0.05$. We report attack success rate, average time and average distortion.

<table>
<thead>
<tr>
<th>METHODS</th>
<th>SUCCESS RATE (%)</th>
<th>AVERAGE TIME (s)</th>
<th>AVERAGE DISTORTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FGM</td>
<td>0</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>BIM/I-FGM</td>
<td>100</td>
<td>99.44</td>
<td>0.0026</td>
</tr>
<tr>
<td>CW</td>
<td>100</td>
<td>722.90</td>
<td>0.0067</td>
</tr>
<tr>
<td>FW-White</td>
<td>100</td>
<td>4.41</td>
<td>0.0045</td>
</tr>
</tbody>
</table>

5.4 Black-box Attack Experiments

In this subsection, we present the black-box experiments on Inception V3 model. For black-box attacks, attack success rate, time needed and number of queries needed are more meaningful evaluation metrics than distortion distances. Therefore, we omit all the grid search / binary search steps that are used in the white-box setting since extra time / queries are needed for finding parameters that can obtain better distortion distances.

Tables 3 and 4 present our experimental results for $L_2$ norm and $L_\infty$ norm based black-box attacks respectively. For ZOO method, note that it only has the $L_2$ norm version and it follows CW’s framework and thus uses different loss function and problem formulation (cannot exactly control the adversarial example to fit the distortion limit, we manage to keep the average distortion around $\epsilon$ for ZOO while other methods have average distortions very close to $\epsilon$). Furthermore, we can observe that ZOO is quite slow in this task. Attack on a single image can take up to 2 hours for ZOO and it is only able to achieve a 74.5% success rate (comparing with the 88.9% success rate in the original paper, we think main cause is the query limit here is only half of the query limit in the origin paper). NES-PGD method, while greatly improving ZOO’s performance, still cannot achieve 100% success rate in both settings and takes relatively more time and queries. In sharp contrast, our proposed Frank-Wolfe black-box attacks (both option I and option II) achieve 100% success rate in both $L_2$ norm and $L_\infty$ norm based attacks and further improve the attack efficiency to another level (around 100s per image for $L_2$ norm case and less than 50s per image for $L_\infty$ norm case).

Table 3: Comparison of $L_2$ norm based black-box attacks on Inception V3 model with $\epsilon = 5$. We report attack success rate, average time and average number of queries needed per image. Opt I and Opt II refer to the two options in Algorithm 2.

<table>
<thead>
<tr>
<th>METHODS</th>
<th>SUCCESS RATE (%)</th>
<th>AVERAGE TIME (s)</th>
<th>AVERAGE QUERIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZOO</td>
<td>74.5</td>
<td>5825.89</td>
<td>294735.87</td>
</tr>
<tr>
<td>NES-PGD</td>
<td>96.5</td>
<td>130.45</td>
<td>58957.55</td>
</tr>
<tr>
<td>FW-Black (Opt I)</td>
<td>100</td>
<td>100.75</td>
<td>45410.50</td>
</tr>
<tr>
<td>FW-Black (Opt II)</td>
<td>100</td>
<td>100.91</td>
<td>44999.75</td>
</tr>
</tbody>
</table>

Table 4: Comparison of $L_\infty$ norm based black-box attacks on Inception V3 model with $\epsilon = 0.05$. We report attack success rate, average time and average number of queries needed per image. Opt I and Opt II refer to the two options in Algorithm 2.

<table>
<thead>
<tr>
<th>METHODS</th>
<th>SUCCESS RATE (%)</th>
<th>AVERAGE TIME (s)</th>
<th>AVERAGE QUERIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>NES-PGD</td>
<td>98</td>
<td>73.58</td>
<td>32741.32</td>
</tr>
<tr>
<td>FW-Black (Opt I)</td>
<td>100</td>
<td>47.56</td>
<td>21129.25</td>
</tr>
<tr>
<td>FW-Black (Opt II)</td>
<td>100</td>
<td>46.48</td>
<td>20694.75</td>
</tr>
</tbody>
</table>

6 Conclusions

In this work, we propose a Frank-Wolfe framework for efficient and effective adversarial attacks. Our proposed white-box and black-box attack algorithms enjoy an $O(1/\sqrt{T})$ rate of convergence, and the query complexity of the proposed black-box attack algorithm is linear in data dimension $d$. Finally, our empirical study on attacking Inception V3 model with ImageNet dataset yields a 100% attack success rate for our proposed algorithms, even in the setting of black-box attack.
**REFERENCES**


Yanpei Liu, Xinyun Chen, Chang Liu, and Dawn Song. Delving into transferable adversarial examples and black-box attacks. *International Conference on Data Mining (ICDM)*, 2018.


A Linear Minimization Oracle (LMO) Solutions

Denote \( u = (v - x_{\text{ori}}) / (\lambda \epsilon) \), the linear minimization problem can be written as

\[
\min_{\|v - x_{\text{ori}}\|_p \leq \lambda \epsilon} (v, \nabla f(x_t, y_{\text{tar}})) = \min_{\|u\|_p \leq 1} \lambda \epsilon \cdot \langle u, \nabla f(x_t, y_{\text{tar}}) \rangle
\]

\[
= \max_{\|u\|_p \leq 1} \lambda \epsilon \cdot \langle u, -\nabla f(x_t, y_{\text{tar}}) \rangle
\]

\[
= \lambda \epsilon \cdot \|\nabla f(x_t, y_{\text{tar}})\|_{p^*},
\]

where \( \|\cdot\|_{p^*} \) denotes the dual norm of \( \|\cdot\|_p \). For \( p = 2 \) case, we have

\[
((v - x_{\text{ori}}) / (\lambda \epsilon), -\nabla f(x_t, y_{\text{tar}})) = \|\nabla f(x_t, y_{\text{tar}})\|_2.
\]

It immediately implies that

\[
v = -\lambda \epsilon \cdot \nabla f(x_t, y_{\text{tar}}) / \|\nabla f(x_t, y_{\text{tar}})\|_2 + x_{\text{ori}}.
\]

For \( p = \infty \) case, we have

\[
((v - x_{\text{ori}}) / (\lambda \epsilon), -\nabla f(x_t, y_{\text{tar}})) = \|\nabla f(x_t, y_{\text{tar}})\|_1.
\]

It immediately implies that

\[
v = -\lambda \epsilon \cdot \text{sign}(\nabla f(x_t, y_{\text{tar}})) + x_{\text{ori}}.
\]

B Proof of the Main Theory in Section 4

B.1 Proof of Theorem 4.3

Proof. For simplicity, we denote \( f(x_t, y_{\text{tar}}) \) by \( f(x_t, y) \) for the rest of the proof. First by Assumption 4.1 we have

\[
\begin{align*}
f(x_{t+1}, y) & \leq f(x_t, y) + \nabla f(x_t, y)^\top (x_{t+1} - x_t) + \frac{L}{2} \|x_{t+1} - x_t\|_2^2 \\
& = f(x_t, y) + \gamma \nabla f(x_t, y)^\top (v_t - x_t) + \frac{L \gamma^2}{2} \|v_t - x_t\|_2^2 \\
& \leq f(x_t, y) + \gamma \nabla f(x_t, y)^\top (v_t - x_t) + \frac{L \gamma^2 2}{2},
\end{align*}
\]

where the last inequality uses the bounded domain condition in Assumption 4.2. Note that by definition of the Frank-Wolfe gap, we have

\[
f(x_{t+1}, y) \leq f(x_t, y) - \gamma g(x_t) + \frac{L \gamma^2 2}{2}.
\]

Do telescope sum over \( t \) of the above inequality, we obtain

\[
f(x_T, y) \leq f(x_0, y) - \sum_{k=0}^{T-1} \gamma g(x_k) + \frac{T L \gamma^2 2}{2}
\]

\[
\leq f(x_0, y) - \gamma T \bar{g}_T + \frac{T L \gamma^2 2}{2},
\]

where the second inequality follows from the definition of \( \bar{g}_T \). Note that by optimality we easily have \( f(x_{t+1}, y) \geq f(x^*, y) \). Rearrange the above inequality we have

\[
\bar{g}_T \leq \frac{f(x_0, y) - f(x^*, y)}{T \gamma} + \frac{L \gamma^2 2}{2}
\]

\[
\leq \sqrt{\frac{L \gamma^2 (f(x_0, y) - f(x^*, y))}{2T}},
\]

where the second inequality is achieved when \( \gamma = \sqrt{2(f(x_0, y) - f(x^*, y))/(L \gamma^2 T)} \).
B.2 PROOF OF LEMMA 4.6

Proof. For simplicity we denote $f(\cdot, y_{h\alpha})$ by $f(\cdot, y)$ for the rest of the proof. Let us denote $\psi_i = \frac{d}{2\delta_i b} (f(x_t + \delta_i u_i, y) - f(x_t - \delta_i u_i, y)) u_i$. For the first part, we have

$$
\mathbb{E}[\psi_i] = \mathbb{E}_u \left[ \frac{d}{2\delta_i b} (f(x_t + \delta_i u_i, y) - f(x_t - \delta_i u_i, y)) u_i \right]
= \mathbb{E}_u \left[ \frac{d}{2\delta_i b} f(x_t + \delta_i u_i, y) u_i \right] + \mathbb{E}_u \left[ \frac{d}{2\delta_i b} f(x_t - \delta_i u_i, y)(-u_i) \right]
= \mathbb{E}_u \left[ \frac{d}{\delta_i b} f(x_t + \delta_i u_i, y) u_i \right]
= \frac{1}{b} \nabla f_\delta(x_t, y),
$$

where the third equality holds due to symmetry of $u_i$ and the last equality follows from Lemma 4.1(a) in [Gao et al., 2018]. Therefore, we have

$$
\mathbb{E}[q_t] = \mathbb{E} \left[ \sum_{i=1}^{b} \psi_i \right] = \nabla f_\delta(x_t, y).
$$

For second part, note that $\psi_i$'s are independent from each other due to the independence of $u_i$, we have

$$
\mathbb{E}\left\|q_t - \mathbb{E}[q_t]\right\|^2 = \mathbb{E}\left\| \sum_{i=1}^{b} \left[ \psi_i - \mathbb{E}\psi_i \right] \right\|^2 = \sum_{i=1}^{b} \mathbb{E}\left\| \psi_i - \mathbb{E}\psi_i \right\|^2 \leq \sum_{i=1}^{b} \mathbb{E}\left\| \psi_i \right\|^2.
$$

Now take a look at $\mathbb{E}\left\| \psi_i \right\|^2$:

$$
\mathbb{E}\left\| \psi_i \right\|^2 = \mathbb{E}_u \left\| \frac{d}{2\delta_i b} (f(x_t + \delta_i u_i, y) - f(x_t, y) + f(x_t, y) - f(x_t - \delta_i u_i, y)) u_i \right\|^2
\leq \frac{1}{2b^2} \mathbb{E}_u \left\| \frac{d}{\delta_i} (f(x_t + \delta_i u_i, y) - f(x_t, y)) u_i \right\|^2 + \frac{1}{2b^2} \mathbb{E}_u \left\| \frac{d}{\delta_i} (f(x_t, y) - f(x_t - \delta_i u_i, y)) u_i \right\|^2
= \frac{1}{b^2} \mathbb{E}_u \left\| \frac{d}{\delta_i} (f(x_t + \delta_i u_i, y) - f(x_t, y)) u_i \right\|^2
\leq \frac{1}{b^2} \left( 2d \left\| \nabla f(x_t, y) \right\|^2 + \frac{1}{2} \delta_i^2 L^2 d^2 \right),
$$

where the first inequality is due to the fact that $(a + b)^2 \leq 2a^2 + 2b^2$, the second equality follows from the symmetry of $u_i$ and the last inequality is by Lemma 4.1(b) in [Gao et al., 2018]. Also note that by Assumption 4.1 and 4.5 we have

$$
\left\| \nabla f(x_t, y) \right\|^2 \leq (\left\| \nabla f(0, y) \right\|^2 + L \left\| x_t \right\|^2) \leq (C_g + LD)^2.
$$

Combine all above results, we obtain

$$
\mathbb{E}\left\|q_t - \mathbb{E}[q_t]\right\|^2 \leq \frac{1}{b} \left( 2d(C_g + LD)^2 + \frac{1}{2} \delta_i^2 L^2 d^2 \right).
$$

\square
B.3 PROOF OF THEOREM 4.7

Proof. For simplicity we denote $f(x_t, y_{\text{hat}}) = f(x_t, y)$ for the rest of the proof. First by Assumption [4.1] we have

$$f(x_{t+1}, y) \leq f(x_t, y) + \nabla f(x_t, y)^\top(x_{t+1} - x_t) + \frac{L}{2} \|x_{t+1} - x_t\|^2_2$$

$$= f(x_t, y) + \gamma \nabla f(x_t, y)^\top(v_t - x_t) + \frac{L\gamma^2}{2} \|v_t - x_t\|^2_2$$

$$\leq f(x_t, y) + \gamma \nabla f(x_t, y)^\top(v_t - x_t) + \frac{LD^2\gamma^2}{2}$$

$$= f(x_t, y) + \gamma q_t^\top(v_t - x_t) + \gamma(\nabla f(x_t, y) - q_t)^\top(v_t - x_t) + \frac{LD^2\gamma^2}{2},$$

where the second inequality uses the bounded domain condition in Assumption 4.2. Now define an auxilary quantity:

$$\tilde{v}_t = \arg\min_{v \in \mathcal{X}} \langle v, \nabla f(x_t, y) \rangle.$$

According to the definition of $g(x_t)$, this immediately implies

$$g(x_t) = \langle \tilde{v}_t, \nabla f(x_t, y) \rangle.$$

Then we further have

$$f(x_{t+1}, y) \leq f(x_t, y) + \gamma q_t^\top(\tilde{v}_t - x_t) + \gamma(\nabla f(x_t, y) - q_t)^\top(\tilde{v}_t - x_t) + \frac{LD^2\gamma^2}{2}$$

$$= f(x_t, y) + \gamma \nabla f(x_t, y)^\top(\tilde{v}_t - x_t) + \gamma(\nabla f(x_t, y) - q_t)^\top(\tilde{v}_t - \tilde{v}_t) + \frac{LD^2\gamma^2}{2}$$

$$= f(x_t, y) - \gamma g(x_t) + \gamma(\nabla f(x_t, y) - q_t)^\top(\tilde{v}_t - \tilde{v}_t) + \frac{LD^2\gamma^2}{2}$$

$$\leq f(x_t, y) - \gamma g(x_t) + \gamma D \cdot \|\nabla f(x_t, y) - q_t\|_2 + \frac{LD^2\gamma^2}{2},$$

where the first inequality follows from the optimally of $v_t$ in Algorithm 2 and the last inequality holds due to Cauchy-Schwarz inequality. Take expectations for both sides of the above inequality, we have

$$E[f(x_{t+1}, y)]$$

$$\leq E[f(x_t, y)] - \gamma E[g(x_t)] + \gamma D \cdot E[\|\nabla f(x_t, y) - q_t\|_2] + \frac{LD^2\gamma^2}{2}$$

$$\leq E[f(x_t, y)] - \gamma E[g(x_t)] + \gamma D \cdot (\|\nabla f(x_t, y) - E[q_t]\|_2 + E[\|q_t - E[q_t]\|_2]) + \frac{LD^2\gamma^2}{2},$$

$$\leq E[f(x_t, y)] - \gamma E[g(x_t)] + \gamma D \cdot (\|\nabla f(x_t, y) - E[q_t]\|_2 + \sqrt{E[\|q_t - E[q_t]\|^2]} + \frac{LD^2\gamma^2}{2})$$

$$\leq E[f(x_t, y)] - \gamma E[g(x_t)] + \gamma D \cdot \left(\|\nabla f(x_t, y) - \nabla f_3(x_t, y)\|_2 + \sqrt{\frac{4d(C_g + LD)^2 + \delta_1^2 L^2 d^2}{2b}}\right)$$

$$+ \frac{LD^2\gamma^2}{2},$$

$$\leq E[f(x_t, y)] - \gamma E[g(x_t)] + \gamma D \cdot \left(\frac{\delta_1 L d}{2} + \frac{2\sqrt{d}(C_g + LD) + \delta_1 L d}{\sqrt{2b}}\right) + \frac{LD^2\gamma^2}{2},$$

where the second inequality follows from triangle inequality, the third inequality is due to Jenson’s inequality and the last inequality holds due to Lemma 4.6.
Do telescope sum over $t$ of the above inequality, we obtain
\[
\mathbb{E}[f(x_T, y)] 
\leq f(x_0, y) - \sum_{t=0}^{T-1} \gamma \mathbb{E}[g(x_t)] + \gamma DT \left( \frac{\delta_t L d}{2} + \frac{2 \sqrt{\delta t (C_g + LD) + \delta_t L d}}{\sqrt{2b}} \right) + \frac{TLD^2 \gamma^2}{2},
\]

where the second inequality follows from the definition of $\tilde{g}_a$. Note that by the zeroth-order optimality, we have $f(x_{t+1}, y) \geq f(x^*, y)$. Rearrange the above inequality we obtain
\[
g_a \leq \frac{f(x_0, y) - f(x^*, y)}{T \gamma} + D \left( \frac{\delta_t L d}{2} + \frac{2 \sqrt{\delta t (C_g + LD) + \delta_t L d}}{\sqrt{2b}} \right)
\]
\[
\leq \frac{D}{\sqrt{2T}} \left( \sqrt{L(f(x_0, y) - f(x^*, y))} + 2(L + C_g + LD) \right),
\]

where the second inequality is achieved by setting $\gamma = \sqrt{2(f(x_0, y) - f(x^*, y))/(LD^2 T)}$, $b = Td$ and $\delta_t = \sqrt{2/Td^2}$.

\[\Box\]

C Parameters Settings for Section 5

For Frank-Wolfe white-box attack algorithm, we list the parameters we use in Section 5 at Table 5.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>$L_2$ CASE</th>
<th>$L_{\infty}$ CASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>${\gamma_t}$</td>
<td>0.03</td>
<td>0.005</td>
</tr>
<tr>
<td>$\lambda$</td>
<td>20</td>
<td>5</td>
</tr>
</tbody>
</table>

Similarly, for Frank-Wolfe black-box attack algorithm, we also list the parameters we use in Section 5 at Table 6.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>$L_2$ CASE</th>
<th>$L_{\infty}$ CASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>$T$</td>
<td>10000</td>
<td>10000</td>
</tr>
<tr>
<td>${\gamma_t}$</td>
<td>0.05/$\sqrt{t}$</td>
<td>0.03/$\sqrt{t}$</td>
</tr>
<tr>
<td>$\lambda$</td>
<td>30</td>
<td>30</td>
</tr>
<tr>
<td>$b$</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>$\delta_t$</td>
<td>0.001</td>
<td>0.01</td>
</tr>
</tbody>
</table>

D Additional Experiments

For the completeness, we also provide some visual illustrations on the adversarial examples generated by various algorithms. Figure 1 shows some examples adversarial examples generated through different $L_2$ norm based white-box attacks. Figure 2 shows some adversarial examples generated through different $L_{\infty}$ norm based black-box attacks.
Figure 1: Sample adversarial examples generated through different $L_2$ norm based white-box attacks. Left side labels denote the original class label and right side labels denote the target class label.
Figure 2: Sample adversarial examples generated through different $L_\infty$ norm based black-box attacks. Left side labels denote the original class label and right side labels denote the target class label.