DeepSearch: Simple and Effective Blackbox Fuzzing of Deep Neural Networks

Fuyuan Zhang
MPI-SWS, Germany
fuyuan@mpi-sws.org

Sankalan Pal Chowdhury
MPI-SWS, Germany
sankalan@mpi-sws.org

Maria Christakis
MPI-SWS, Germany
maria@mpi-sws.org

ABSTRACT

Although deep neural networks have been successful in image classification and image recognition, they are prone to adversarial attacks. To generate misclassified inputs, there has emerged a wide variety of techniques, such as black- and whitebox testing of neural networks. In this paper, we present DeepSearch, a novel blackbox-fuzzing technique for image classifiers. Despite its simplicity, DeepSearch is shown to be more effective in finding adversarial examples than closely related black- and whitebox approaches. DeepSearch is additionally able to generate the most subtle adversarial examples in comparison to these approaches.

1 INTRODUCTION

Deep neural networks have been impressively successful in pattern recognition and image classification [30, 38, 41]. However, the more popular deep neural networks become for performing such tasks, the more incentives adversaries have for trying to trick them into making a wrong prediction, often with critical consequences. In fact, even very subtle perturbations of a correctly classified image, perhaps imperceptible to the human eye, may cause a deep neural network to change its prediction [68].

More formally, let \( \mathbb{R}^n \) be the \( n \)-dimensional vector space for input images. We represent images as column vectors \( \mathbf{x} = (x_1, \ldots, x_n)^T \), where \( x_i \in \mathbb{R} (1 \leq i \leq n) \) is the \( i \)th coordinate of \( \mathbf{x} \). We also write \( \mathbf{x}(i) \) to denote the \( i \)th coordinate \( x_i \), i.e., \( \mathbf{x}(i) = x_i \), and each such coordinate represents an image pixel. Now, let \( C_m = \{l_1, \ldots, l_m\} \) be a set of labels for \( m \) classes, where \( l_i \) is the label for the \( i \)th class \( (1 \leq i \leq m) \). A deep neural network that classifies images from \( \mathbb{R}^n \) into \( m \) classes in \( C_m \) is essentially a function \( N : \mathbb{R}^n \rightarrow C_m \). For an input \( \mathbf{x} \in \mathbb{R}^n \), \( N(\mathbf{x}) \) is the label that the network assigns to \( \mathbf{x} \).

Assume that input \( \mathbf{x} \) is correctly classified, and \( \mathbf{x}' \) is generated by applying subtle perturbations to \( \mathbf{x} \). These perturbations are subtle when the distance between \( \mathbf{x} \) and \( \mathbf{x}' \) in \( \mathbb{R}^n \) is sufficiently small according to a distance metric. When this is so and \( N(\mathbf{x}) \neq N(\mathbf{x}') \), we say that \( \mathbf{x}' \) is an adversarial example [68]. In other words, the network is tricked into classifying \( \mathbf{x}' \) into a different class than \( \mathbf{x} \) even though they are very similar.

In this paper, we use the \( L_\infty \) distance metric. The \( L_\infty \) distance between \( \mathbf{x} \) and \( \mathbf{x}' \) is defined as the maximum of their differences along any coordinate dimension \( 1 \leq i \leq n \):

\[
||\mathbf{x} - \mathbf{x}'||_{L_\infty} = \max_i (|x_i - x'_i|)
\]

For \( d \in \mathbb{R} \), we write \( B(\mathbf{x}, d) \) to denote the set of images within distance \( d \) from \( \mathbf{x} \), i.e., \( B(\mathbf{x}, d) = \{ \mathbf{x}' | ||\mathbf{x} - \mathbf{x}'||_{L_\infty} \leq d \} \), which is an \( n \)-dimensional cube.

Based on the above, a deep neural network \( N \) is locally robust for a correctly classified input \( \mathbf{x} \) with respect to distance \( d \) if it assigns the same label to all images in \( B(\mathbf{x}, d) \). There have recently emerged numerous approaches for evaluating local robustness of a deep neural network. Whitebox techniques have full access to the network under evaluation (e.g., [12, 24, 39, 56]). On the other hand, blackbox techniques may only query the network for its predictions on particular inputs (e.g., [5, 6, 51]). In other words, such techniques may only observe the input-output behavior of the network and assume no knowledge about the network structure or its parameters.

Recently, Wicker et al. [74] proposed a blackbox technique for testing image classifiers. They first extract features from images and then encode the problem of finding adversarial examples as a two-player turn-based stochastic game. Although competitive with state-of-the-art whitebox techniques, this approach is very complicated. Inspired by the linear explanation of adversarial examples [24], we develop a simple, yet very effective, blackbox-fuzzing technique for deep neural networks.

Our approach. We present DeepSearch, a blackbox-fuzzing technique for testing the robustness of deep neural networks for image classification. DeepSearch is a novel blackbox approach that does not apply gradient-based methods. Starting from a correctly classified input image \( \mathbf{x} \), DeepSearch strategically mutates its pixels to values that are more likely to lead to an adversarial example \( \mathbf{x}' \). Once such an example is found, DeepSearch is able to significantly reduce its distance from \( \mathbf{x} \), thereby finding subtle adversarial examples generated by only slightly perturbing pixels in \( \mathbf{x} \).

Not only does DeepSearch use a fundamentally novel technique for testing neural networks, but it is also shown to be more effective in generating adversarial examples than state-of-the-art black- and whitebox approaches. Moreover, in comparison to these related approaches, DeepSearch is able to find the most subtle adversarial examples on two popular image datasets, namely MNIST [42] and CIFAR-10 [37].

Contributions. We make the following contributions:

(1) We present a simple, yet very effective, blackbox-fuzzing technique for deep neural networks.

(2) We perform an extensive evaluation showing that DeepSearch is more effective in finding adversarial examples than state-of-the-art black- and whitebox approaches.

(3) We show that a straightforward extension to our technique, which we call refinement, gives DeepSearch the advantage of finding the most subtle adversarial examples in comparison to related approaches.

Outline. The following section presents DeepSearch for finding adversarial examples in binary classifiers, that is, networks that classify inputs into two classes. Sect. 3 generalizes the technique to multiclass classifiers, which classify inputs into multiple classes. In
2 FUZZING BINARY CLASSIFIERS

In this section, we present the technical details of how DeepSearch fuzzes (linear and non-linear) binary classifiers.

2.1 Linear Binary Classifiers

In the following, we rely on background on linear binary classifiers, give an intuition on how our technique fuzzes their inputs through an example, and present our methodology in detail.

Background. A binary classifier classifies inputs into two classes, denoted with labels $C_2 = \{l_1, l_2\}$, according to the definition below.

**Definition 1 (Binary Classifier).** Given a classification function $f : \mathbb{R}^n \to \mathbb{R}$, a binary classifier $N_f : \mathbb{R}^n \to C_2$ is defined as follows:

$$ N_f(x) = \begin{cases} l_1, & \text{if } f(x) > 0 \\ l_2, & \text{if } f(x) < 0 \end{cases} $$

If function $f$ is linear, then $N_f$ is a linear binary classifier, otherwise it is non-linear.

The set of values $D_f = \{x \mid f(x) = 0\}$ constitute the decision boundary of $N_f$, which classifies the domain $\mathbb{R}^n$ into the two classes in $C_2$. As an example, consider Fig. 1a, showing a linear binary classifier $N_f : \mathbb{R}^2 \to C_2$. (The red dashed and dash-dotted lines should be ignored for now.) Observe that input $x_0$ is classified in $l_1$ whereas $x'_0$ is in $l_2$. Note that the decision boundary of a linear classifier $N_f : \mathbb{R}^n \to C_2$ is a hyperplane; it is, therefore, a straight line in Fig. 1a.

Given a binary classifier $N_f$ and a correctly classified input $x$, there exists an adversarial example in the set of inputs within distance $d \in \mathbb{R}$ of $x$, denoted $B(x, d)$, if and only if another input $x' \in B(x, d)$ is classified differently than $x$. In other words, $x'$ is an adversarial example if $N_f(x') \neq N_f(x)$, which is equivalent to $f(x)f(x') < 0$. For example, assume that input $x_0 = (x_h, x_v)$ in Fig. 1a is correctly classified and that the dash-dotted square represents $B(x, d)$. Then, $x'_0$ is an adversarial example.

**Example.** We give an intuition on how DeepSearch handles linear binary classifiers using the example of Fig. 1a. Recall that $x_0$ is a correctly classified input for which $f(x_0) > 0$. To find an adversarial example, DeepSearch fuzzes $x_0$ with the goal of generating a new input $x'_0$ such that $f(x'_0) < 0$.

Fuzzing is performed as follows. Input $x_0$ has two coordinates $x_h$ and $x_v$, for the horizontal and vertical dimensions. DeepSearch independently mutates each of these coordinates to the minimum and maximum values that are possible within $B(x_0, d)$, with the intention to find the minimum value of $f$ on $B(x_0, d)$. For instance, when mutating $x_h$, we obtain inputs $x_0[l_h, x_h]$ and $x_0[u_h, x_h]$ in the figure. Values $l_h$ and $u_h$ are, respectively, the minimum and maximum that $x_h$ may take, and $x_0[l_h, x_h]$ denotes substituting $x_h$ with $l_h$ (similarly for $x_0[u_h, x_h]$). We then evaluate $f(x_0[l_h, x_h])$ and $f(x_0[u_h, x_h])$, and for $x_h$, we select the value ($l_h$ or $u_h$) that causes function $f$ to decrease. This is, in our example, an adversarial input $x'_0$ must make the value of $f$ negative. Let us assume that $f(x_0[l_h, x_h]) < f(x_0[l_h, x_h])$, we, thus, select $u_h$ for coordinate $x_h$.

DeepSearch mutates coordinate $x_v$ in a similar way. It evaluates $f(x_0[l_v, x_v])$ and $f(x_0[u_v, x_v])$, and selects the value that causes $f$ to decrease. Let us assume that $f(x_0[l_v, x_v]) < f(x_0[l_v, x_v])$, we, thus, select $u_v$ for $x_v$.

Next, we generate input $x'_0$ by substituting each coordinate in $x_0$ with the boundary value that was previously selected. In other words, $x'_0 = x_0[u_h, x_h, u_v, x_v]$, and since $f(x'_0) < 0$, DeepSearch has generated an adversarial example. Note that $f(x'_0)$ is actually the minimum value of $f$ on $B(x_0, d)$.

**DeepSearch for linear binary classifiers.** We now formalize how DeepSearch treats linear binary classifiers. Consider a linear classification function $f(x) = \mathbf{w}^T x + b = \sum_{i=1}^n w_i x_i + b$, where $\mathbf{w}^T = (w_1, ..., w_n)$ and $b \in \mathbb{R}$. Note that $f$ is monotonic with respect to all of its variables $x_1, ..., x_n$. For instance, if $w_i > 0$, then $f$ is monotonically increasing in $x_i$.

Recall that $B(x, d)$ denotes the set of inputs within distance $d \in \mathbb{R}$ of an input $x$. $B(x, d)$ may be represented by an $n$-dimensional cube $I = l_1 \times \cdots \times l_n$, where $l_i = [l_i, u_i]$ is a closed interval bounded by $l_i, u_i \in \mathbb{R}$ with $l_i \leq u_i$ for $1 \leq i \leq n$. Intuitively, value $l_i$ (resp. $u_i$) is the lower (resp. upper) bound on the $i$th dimension of $x$. An input $x'$ is a vertex of $I$ if each of its coordinates $x'(i)$ is an endpoint of $l_i$ for $1 \leq i \leq n$, i.e., $x'(i) = u_i$ or $l_i$ ($1 \leq i \leq n$).

We write $f(I)$ for the values of $f$ on $I$: $f(I) = \{f(x) \mid x \in I\}$. Due to the monotonicity of $f$, the maximum and minimum values of $f$ on $I$ may be easily calculated by applying $f$ to vertices of $I$:

**Theorem 1.** Given a linear classification function $f(x) = \mathbf{w}^T x + b$, where $\mathbf{w}^T = (w_1, ..., w_n)$ and $b \in \mathbb{R}$, an $n$-dimensional cube $I = l_1 \times \cdots \times l_n$, where $l_i = [l_i, u_i]$ for $1 \leq i \leq n$, and an input $x \in I$, we have:

1. $\min f(I) = f(x')$, where $x'(i) = l_i$ (resp. $x'(i) = u_i$) if $f(x[u_i/x_i]) > f(x[l_i/x_i])$ (resp. $f(x[u_i/x_i]) \leq f(x[l_i/x_i])$) for $1 \leq i \leq n$
2. $\max f(I) = f(x')$, where $x'(i) = u_i$ (resp. $x'(i) = l_i$) if $f(x[u_i/x_i]) > f(x[l_i/x_i])$ (resp. $f(x[u_i/x_i]) \leq f(x[l_i/x_i])$) for $1 \leq i \leq n$

As above, we can precisely calculate the minimum and maximum values of $f$ in any $n$-dimensional cube. In particular, assume a correctly classified input $x$ for which $f(x) > 0$. For any dimension $i$ ($1 \leq i \leq n$) of $x$, we first construct inputs $x[l_i/x_i]$ and $x[u_i/x_i]$. We then compare the values of $f(x[l_i/x_i])$ and $f(x[u_i/x_i])$. To generate a new input $x'$, we select the value of its $i$th coordinate as follows:

$$ x'(i) = \begin{cases} l_i, & \text{if } f(x[u_i/x_i]) > f(x[l_i/x_i]) \\ u_i, & \text{if } f(x[u_i/x_i]) \leq f(x[l_i/x_i]) \end{cases} $$

As shown here, selecting a value for $x'(i)$ requires evaluating function $f$ twice, i.e., $f(x[l_i/x_i])$ and $f(x[u_i/x_i])$. Therefore, for $n$ dimensions, $f$ must be evaluated $2n$ times. In practice however, due to the monotonicity of $f$, evaluating it only once per dimension is sufficient. For instance, if $f(x[u_i/x_i])$ already decreases (resp. increases) the value of $f$ in comparison to $f(x)$, there is no need to evaluate $f(x[u_i/x_i])$. Value $u_i$ (resp. $l_i$) should be selected for the $i$th coordinate. Hence, the minimum value of $f$ can be computed.
by evaluating the function exactly $n$ times. If, for the newly generated input $x'$, the sign of $f$ becomes negative, $x'$ constitutes an adversarial example.

We treat the case where $f(x) < 0$ for a correctly classified input $x$ analogously. DeepSearch aims to generate a new input $x'$ such that the sign of $f$ becomes positive. We are, therefore, selecting coordinate values that cause $f$ to increase.

### 2.2 Non-Linear Binary Classifiers

We generalize our technique to non-linear binary classifiers. In this setting, DeepSearch iteratively approximates the minimum and maximum values of $f$ in $B(x, d)$.

**Example.** As an example, consider the non-linear classification function $f$ shown in Fig. 1b. Since $f$ is non-linear, the decision boundary $D_f$ of the binary classifier is a curve.

Starting from correctly classified input $x_0$, DeepSearch treats $f$ as linear within $B(x_0, d)$ and generates $x_1$, exactly as it would for a linear binary classifier. Observe that input $x_1$ is not adversarial. Unlike for a linear binary classifier however, where the minimum value of $f$ in $B(x_0, d)$ is precisely computed, the non-linear case is handled by iteratively approximating the minimum. In particular, after generating $x_1$, DeepSearch iterates starting from $x_1$, while again treating $f$ as linear in $B(x_0, d)$. As a result, our technique generates input $x_k$, which is adversarial.

**DeepSearch for non-linear binary classifiers.** Alg. 1 shows DeepSearch for binary classifiers. It uses iterative approximations to search for adversarial examples. Note that our technique is blackbox, and consequently, it cannot differentiate between linear and non-linear classifiers. Alg. 1 is, therefore, the general algorithm that DeepSearch applies to fuzz any binary classifier.

The main function in Alg. 1 is $DS$-Binary. Input $x_{init}$ is the input from which we start the first iteration, e.g., it corresponds to $x_0$ in Fig. 1. Input $x$ is used to compute $B(x, d)$, and for now, assume that $x$ is equal to $x_{init}$. (We will discuss why $x$ is needed in Sect. 4.) In addition to these inputs, the algorithm also takes a classification function $f$ and the distance $d$. If it terminates, it returns an adversarial example $x'$.

Function $DS$-Binary first assigns $x_{init}$ to $x_0$ and constructs $n$ intervals $I_1, ..., I_n$ to represent $B(x_0, d)$ (lines 20–21). Then, based on the sign of $f(x_0)$, our algorithm iteratively approximates the minimum (lines 23–26) or the maximum (lines 28–31) value of $f$ in $B(x_0, d)$. Each iteration evaluates $f$ 2$n$ times (see Sect. 2.1). $DS$-Binary terminates when an adversarial example is found. If such an example is found in $k$ iterations, we evaluate $f$ $2nk$ times. Note that, in practice, we set a bound on the number of iterations, which we discuss in Sect. 5.

Algorithm 1: DeepSearch for binary classifiers.

**Input:** input $x \in \mathbb{R}^n$, initial input $x_{init} \in B(x, d)$, function $f : \mathbb{R}^n \rightarrow \mathbb{R}$, distance $d \in \mathbb{R}$

**Output:** an adversarial input $x'$

**Function $\text{ApproxMax}(x, f, (I_1, ..., I_n))$ is**

1. $x' := (0, ..., 0)$
2. $\text{foreach } 1 \leq i \leq n \text{ do}$
3. 3. $\text{if } f(x[I_i/x_i]) > f(x[I_i/x_i]) \text{ then}$
4. 4. $x' := x'[I_i/x_i']$
5. 5. else
6. 6. $x' := x'[I_i/x_i']$
7. 7. $\text{return } x'$
8. $\text{end foreach}$
9. $\text{end function}$

**Function $\text{ApproxMin}(x, f, (I_1, ..., I_n))$ is**

1. $x' := (0, ..., 0)$
2. $\text{foreach } 1 \leq i \leq n \text{ do}$
3. 3. $\text{if } f(x[I_i/x_i]) < f(x[I_i/x_i]) \text{ then}$
4. 4. $x' := x'[I_i/x_i']$
5. 5. else
6. 6. $x' := x'[I_i/x_i']$
7. 7. $\text{return } x'$
8. $\text{end foreach}$
9. $\text{end function}$

**Function $DS$-Binary($x$, $x_{init}$, $f$, $d$) is**

1. construct intervals $(I_1, ..., I_n)$ such that $B(x, d) = I_1 \times ... \times I_n$
2. initialize $x_0 := x_{init}$ and $k := 0$
3. $\text{if } f(x_0) > 0 \text{ then}$
4. 4. $\text{repeat}$
5. 5. $\text{if } f(x[I_i/x_i]) > f(x[I_i/x_i]) \text{ then}$
6. 6. $x_{k+1} := \text{ApproxMin}(x_k, f, (I_1, ..., I_n))$
7. 7. $k := k + 1$
8. 8. $\text{until } x_k \text{ is an adversarial example}$
9. 9. $\text{else}$
10. 10. $\text{repeat}$
11. 11. $\text{if } f(x[I_i/x_i]) < f(x[I_i/x_i]) \text{ then}$
12. 12. $x_{k+1} := \text{ApproxMax}(x_k, f, (I_1, ..., I_n))$
13. 13. $k := k + 1$
14. 14. $\text{until } x_k \text{ is an adversarial example}$
15. 15. $\text{return } x_k$
16. $\text{end else}$

Figure 1: DeepSearch for binary classifiers.
3 FUZZING MULTICLASS CLASSIFIERS

In this section, we extend our technique for blackbox fuzzing of binary classifiers to multiclass classifiers.

3.1 Linear Multiclass Classifiers

Background. A multiclass classifier classifies inputs in \( m \) classes according to the following definition.

**Definition 2 (Multiclass Classifier).** For classification function \( f : \mathbb{R}^n \rightarrow \mathbb{R}^m \), which returns \( m \) values each corresponding to one class in \( C_m = \{1, \ldots, m\} \), a multiclass classifier \( N_f : \mathbb{R}^n \rightarrow C_m \) is defined as

\[
N_f(x) = l_j, \quad \text{if } j = \arg \max_i f_i(x),
\]

where \( f_i : \mathbb{R}^n \rightarrow \mathbb{R} \) denotes the function derived by evaluating \( f \) for the \( i \)-th class, i.e., \( f(x) = (f_1(x), \ldots, f_m(x))^T \).

In other words, a multiclass classifier \( N_f \) classifies an input \( x \) in \( l_j \) if \( f_j(x) \) evaluates to the largest value in comparison to all other functions \( f_i \).

Function \( f \) of a multiclass classifier \( N_f \) may be decomposed into multiple binary classifiers such that the original multiclass classifier may be reconstructed from these binary classifiers. First, to decompose a multiclass classifier into binary classifiers, for any pair of classes \( l_i, l_j \) (\( 1 \leq i, j \leq m \)), we define a classification function \( g_{ij} : \mathbb{R}^n \rightarrow \mathbb{R} \) as \( g_{ij}(x) = f_i(x) - f_j(x) \). We then construct a binary classifier \( N_{g_{ij}} : \mathbb{R}^n \rightarrow \{l_i, l_j\} \) as follows:

\[
N_{g_{ij}}(x) = \begin{cases} 
  l_i, & \text{if } g_{ij}(x) > 0 \\
  l_j, & \text{if } g_{ij}(x) < 0
\end{cases}
\]

As usual, the set of values \( D_{g_{ij}} = \{x \mid f_i(x) - f_j(x) = 0\} \) constitutes the pairwise decision boundary of binary classifier \( N_{g_{ij}} \), which classifies the domain \( \mathbb{R}^n \) into the two classes \( l_i, l_j \). As an example, consider Fig. 2a depicting a multiclass classifier \( N_f : \mathbb{R}^2 \rightarrow C_3 \), where \( f \) is linear and \( C_3 = \{l_1, l_2, l_3\} \). Assume that \( N_f \) correctly classifies input \( x \) in \( l_2 \). Based on the above, linear binary classifiers are a linear combination of binary classifiers as follows. An input \( x \) is classified in class \( l_i \) by multiclass classifier \( N_f \) if and only if it is classified in \( l_i \) by all \( m \) binary classifiers \( N_{g_{ij}} \) for \( 1 \leq j \leq m, i \neq j \), where \( l_i \in C_m \) and \( g_{ij}(x) = f_i(x) - f_j(x) \):

\[
N_f(x) = l_i, \quad \text{if } \forall 1 \leq j \leq m, i \neq j : N_{g_{ij}}(x) = l_i
\]

For instance, in Fig. 2a, if both \( N_{g_{12}} \) and \( N_{g_{13}} \) classify input \( x \) in class \( l_2 \), then the multiclass classifier also classifies it in \( l_2 \).

Based on the above, a multiclass classifier has an adversarial input if and only if this input is also adversarial for a constituent binary classifier:

**Corollary 1.** Let \( N_f \) be a multiclass classifier and \( x \in \mathbb{R}^n \) a correctly classified input, where \( N_f(x) = l_i \) and \( l_i \in C_m \). There exists an adversarial example \( x' \in B(x, d) \) for \( N_f \), where \( d \in \mathbb{R} \), if and only if \( x' \) is an adversarial example for a binary classifier \( N_{g_{ij}}(1 \leq j \leq m, i \neq j) \), where \( g_{ij}(x) = f_i(x) - f_j(x) \):

\[
N_f(x') \neq l_i, \quad \text{iff } \exists 1 \leq j \leq m, i \neq j : N_{g_{ij}}(x') \neq l_i
\]

Let us consider again the example of Fig. 2a. Recall that multiclass classifier \( N_f \) correctly classifies input \( x \) in class \( l_2 \), and so do binary classifiers \( N_{g_{12}} \) and \( N_{g_{13}} \).

**Example.** This corollary is crucial in generalizing our technique to multiclass classifiers. Assume a correctly classified input \( x \), for which \( N_f(x) = l_i \). According to the above corollary, the robustness of \( N_f \) in \( B(x, d) \) reduces to the robustness of all \( m - 1 \) binary classifiers \( N_{g_{ij}} \) (\( 1 \leq j \leq m, i \neq j \)) in \( B(x, d) \). We, therefore, use DeepSearch for binary classifiers to test each binary classifier in this set. If there exists an adversarial input \( x' \) for one of these classifiers, i.e., \( N_{g_{ij}}(x') \neq l_i \) for some \( j \), then \( x' \) is also an adversarial input for \( N_f \), i.e., \( N_f(x') \neq l_i \).

Let us consider the example of Fig. 2a. Recall that multiclass classifier \( N_f \) correctly classifies input \( x \) in class \( l_2 \), and so do binary classifiers \( N_{g_{12}} \) and \( N_{g_{13}} \).

**DeepSearch for linear multiclass classifiers.** Let us assume a linear classification function \( f(x) = W^T x + b \), where \( W^T = (w_{11}, \ldots, w_{m1})^T \), \( w_1 \in \mathbb{R}^n \) (\( 1 \leq i \leq m \)), and \( b = (b_1, \ldots, b_m)^T \in \mathbb{R}^m \). Then, \( f_i \), which denotes the function derived by evaluating \( f \) for the \( i \)-th class, is of the form \( f_i(x) = w_i^T x + b_i \) for \( 1 \leq i \leq m \). For any pair of class labels \( l_i, l_j \), function \( g_{ij} \) is defined as \( g_{ij}(x) = f_i(x) - f_j(x) = (w_i^T - w_j^T) x + (b_i - b_j) \). Hence, \( g_{ij} \) is also linear, and \( N_{g_{ij}} \) is a linear binary classifier.

Assume that classifier \( N_f \) correctly classifies input \( x \in \mathbb{R}^n \) in \( l_i \), \( N_f(x) = l_i \) \( (l_i \in C_m) \). According to Cor. 1, the robustness of \( N_f \) in \( B(x, d) \) reduces to the robustness of each binary classifier \( N_{g_{ij}} \) (\( 1 \leq j \leq m, i \neq j \)) in \( B(x, d) \). To find an adversarial example for a binary classifier \( N_{g_{ij}} \) in \( B(x, d) \), DeepSearch must generate an input \( x' \in B(x, d) \) such that \( g_{ij}(x') < 0 \). (Recall that by definition \( g_{ij}(x) > 0 \).)

DeepSearch for linear multiclass classifiers. Let us assume a linear classification function \( f(x) = W^T x + b \), where \( W^T = (w_{11}, \ldots, w_{m1})^T \), \( w_1 \in \mathbb{R}^n \) (\( 1 \leq i \leq m \)), and \( b = (b_1, \ldots, b_m)^T \in \mathbb{R}^m \). Then, \( f_i \), which denotes the function derived by evaluating \( f \) for the \( i \)-th class, is of the form \( f_i(x) = w_i^T x + b_i \) for \( 1 \leq i \leq m \). For any pair of class labels \( l_i, l_j \), function \( g_{ij} \) is defined as \( g_{ij}(x) = f_i(x) - f_j(x) = (w_i^T - w_j^T) x + (b_i - b_j) \). Hence, \( g_{ij} \) is also linear, and \( N_{g_{ij}} \) is a linear binary classifier.
Algorithm 2: DeepSearch for multiclass classifiers.

Input: input $x \in \mathbb{R}^n$, initial input $x_{init} \in \mathcal{B}(x, d)$, function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$, distance $d \in \mathbb{R}$

Output: an adversarial input $x'$

1. **Function DS-Multiclass($x$, $x_{init}$, $f$, $d$) is**
   2. construct intervals $(l_1, \ldots, l_n)$ such that $\mathcal{B}(x, d) = l_1 \times \ldots \times l_n$
   3. $l_i := N_f(x)$
   4. define functions $g_{ij}(x) = f_j(x) - f_i(x)$, $1 \leq j \leq m$, $i \neq j$
   5. initialize $x_0 := x_{init}$ and $k := 0$
   6. repeat
      7. $r := \arg\min_j g_{ij}(x_k)$
      8. $x_{k+1} := \text{ApproxMin}(x_k, g_{ir}(l_1, \ldots, l_n))$
      9. $k := k + 1$
   10. until $x_k$ is an adversarial example
   11. return $x_k$

function $g_{ij}$ is defined as $g_{ij}(x) = f_j(x) - f_i(x)$, where $f_i(x)$ and $f_j(x)$ are the values of $f(x)$ for the $i$th and $j$th classes, respectively. If the sign of $g_{ij}(x')$ becomes negative for some $j$, then DeepSearch has found an adversarial example for $N_f$ in $\mathcal{B}(x, d)$.

### 3.2 Non-Linear Multiclass Classifiers

We now extend our technique to non-linear multiclass classifiers. Analogously to Sect. 2.2, DeepSearch iteratively approximates the minimum values of functions $g_{ij}$ in $\mathcal{B}(x, d)$.

**Example.** As an example, consider Fig. 2b depicting a multiclass classifier $N_f : \mathbb{R}^2 \rightarrow C_3$, where $f$ is non-linear and $C_3 = \{l_1, l_2, l_3\}$. Assume that $N_f$ classifies input $x_0$ in class $l_2$, and thus, do non-linear binary classifiers $N_{g_{21}}$ and $N_{g_{23}}$.

Let us also assume that $g_{21}(x_0) < g_{23}(x_0)$. Since $g_{21}$ evaluates to a smaller value than $g_{23}$ for input $x_0$, we consider it more likely to have an adversarial example. In other words, we first approximate the minimum value of $g_{21}$ because it is closer to becoming negative for the initial input. DeepSearch treats $g_{21}$ as linear within $\mathcal{B}(x_0, d)$ and generates $x_1$. Observe that input $x_1$ is not adversarial. Now, assume that $g_{21}(x_1) > g_{23}(x_1)$. As a result, DeepSearch tries to find the minimum of function $g_{23}$ in $\mathcal{B}(x_0, d)$, also by treating it as linear. It generates input $x_2$, which is an adversarial example for classifiers $N_{g_{23}}$ and $N_f$.

DeepSearch for non-linear multiclass classifiers. Alg. 2 is the general DeepSearch algorithm for multiclass problems. The inputs are the same as for Alg. 1. For now, assume that $x$ is equal to $x_{init}$. Again, if the algorithm terminates, it returns an adversarial example for $N_f$ in $\mathcal{B}(x, d)$.

Function $DS-$Multiclass assigns $x_{init}$ to $x_0$ and constructs $n$ intervals $l_1, \ldots, l_n$ to represent $\mathcal{B}(x_0, d)$. It also computes the class label $l_1$ of $x_0$, and defines functions $g_{ij} (1 \leq j \leq m, i \neq j)$ (lines 2–5). The rest of the algorithm uses ApproxMin from Alg. 1 to iteratively approximate the minimum of one function $g_{ij}$ per iteration. This function is selected on line 7 such that its value for input $x_k$ is smaller in comparison to all other constituent binary classification functions. This heuristic allows our algorithm to find an adversarial example faster than having to generate an input $x_{k+1}$ for all $m - 1$ functions $g_{ij}$ per iteration. $DS-$Multiclass terminates when an adversarial example is found. If such an example is found in $k$ iterations, we evaluate $f$ 2nk times.

### 4 FUZZING WITH ITERATIVE REFINEMENT

The closer the adversarial examples are to a correctly classified input, the more subtle they are. Such adversarial examples are said to have a low distortion rate. In this section, we extend DeepSearch with an iterative refinement approach for finding subtle adversarial examples. On a high level, given an input $x$ and a distance $d$, for which we have already found an adversarial example $x'$ in region $\mathcal{B}(x, d)$, DeepSearch iteratively reduces distance $d$ as long as the smaller region still contains an adversarial example. If none is found, the distance is not reduced further.

**Background.** Let $I = l_1 \times \ldots \times l_n$ be an $n$-dimensional cube, where $l_i = [u_i, u_i]$ is a closed interval bounded by $l_i, u_i \in \mathbb{R}$ with $l_i \leq u_i$ for $1 \leq i \leq n$. For an input $x$ with an $i$th coordinate $x(i) \in (-\infty, l_i] \cup [u_i, +\infty)$ for $1 \leq i \leq n$, we define a projection operator $\text{Proj}$ that maps $x$ to a vertex of $I$ as follows.

$$\text{Proj}(I, x)(i) = \begin{cases} u_i, & \text{if } x(i) \geq u_i \\ l_i, & \text{if } x(i) \leq l_i. \end{cases}$$

where $\text{Proj}(I, x)(i)$ denotes the $i$th coordinate of $\text{Proj}(I, x)$. As an example, consider Fig. 3a showing a linear multiclass classifier. Input $x_2$ is a projection of $x_1$.

Using the above projector operator, the minimum and maximum values of a linear classification function $f$ may also be projected on $I$. In particular:

**Theorem 2.** Let $f(x) = w^T x + b$ be a linear classification function, and $I_1, I_2$ two $n$-dimensional cubes such that $I_1 \subseteq I_2$. Assuming that $x$ is an input for which $f$ obtains its minimum or maximum value in $I_2$, we have:

1. if $\min f(I_2) = f(x)$, then $\min f(I_1) = f(\text{Proj}(I_1, x))$
2. if $\max f(I_2) = f(x)$, then $\max f(I_1) = f(\text{Proj}(I_1, x))$

In Fig. 3a, assume that input $x_0$ is correctly classified in class $l_2$. Then, in region $\mathcal{B}(x_0, d_1)$, function $g_{23}$ obtains its minimum value for input $x_1$. When projecting $x_1$ to vertex $x_2$ of $\mathcal{B}(x_0, d_2)$, notice that $g_{23}$ evaluates to its minimum value for input $x_2$ in this smaller region.

**Example.** Fig. 3 shows two multiclass classifiers $N_f : \mathbb{R}^2 \rightarrow C_3$, where $C_3 = \{l_1, l_2, l_3\}$. In Fig. 3a, function $f$ is linear, whereas in Fig. 3b, it is non-linear. For correctly classified input $x_0$, we assume that $N_f(x_0) = l_2$, and thus, $N_{g_{23}}(x_0) = l_2$ and $N_{g_{21}}(x_0) = l_2$.

In both subfigures, assume that $x_1$ is an adversarial example found by DS-Multiclass (see Alg. 2) in $\mathcal{B}(x_0, d_1)$. Once such an example is found, our technique with refinement uses bisect search to find the smallest distance $d'$ such that the projection of $x_1$ on $\mathcal{B}(x_0, d')$ is still adversarial. In Fig. 3, this distance is $d_2$, and input $x_2$ constitutes the projection of $x_1$ on $\mathcal{B}(x_0, d_2)$. So, $x_2$ is closer to $x_0$, which means that it has a lower distortion rate than $x_1$. In fact, since we are using bisect search to determine distance $d_2$, $x_2$ is the closest adversarial input to $x_0$ that may be generated by projecting $x_1$ on smaller regions.

However, in region $\mathcal{B}(x_0, d_2)$, there may be other vertices that are adversarial and get us even closer to $x_0$ with projection. To find such examples, we apply DS-Multiclass again, this time starting from input $x_2$ and searching in region $\mathcal{B}(x_0, d_2)$. As a result, we...
generate adversarial input $x_3$ in the subfigures. Now, by projecting $x_3$ to the smallest possible region around $x_0$, we compute $x_4$, which is the adversarial example with the lowest distortion rate so far.

Assume that applying DS-Multiclass for a third time, starting from $x_4$ and searching in $B(x_0, d_3)$, does not generate any other adversarial examples. In this case, our technique returns $x_4$.

**DeepSearch with iterative refinement.** Alg. 3 describes our technique with iterative refinement. Each iteration consists of a refinement and a search step, which we explain next.

The refinement step (lines 3–4) first calculates the $L_\infty$ distance $d$ between $x$ and $x'$. In Fig. 3, input $x$ of the algorithm is $x_0$, and $x'$ is $x_1$. So, $x'$ is an adversarial input that was generated by our technique, and consequently, a vertex of $B(x, d)$. On line 4, we use bisect search to find the minimum distance $d'$ such that the input derived by projecting $x'$ on $B(x, d')$ is still adversarial. In Fig. 3, this is distance $d_2$, and $\text{Proj}(B(x, d'), x')$ of the algorithm corresponds to adversarial input $x_2$ in the figure.

Note that this refinement is possible because of Thm. 2, which guarantees that a linear function $f$ evaluates to its minimum in $B(x, d')$ for the input derived with projection. When $f$ is non-linear, it might not evaluate to its minimum for adversarial input $\text{Proj}(B(x, d'), x)$. However, it is still the case that this projected input is closer to $x$, i.e., $||x - \text{Proj}(B(x, d')||_\infty \leq ||x - x'||_\infty$, and thus, has a lower distortion rate.

The search step (lines 5–8) calls function $\text{DS-Binary}$ (Alg. 1) or $\text{DS-Multiclass}$ (Alg. 2), depending on whether $f$ is a binary classification function. The goal is to search for another adversarial example (other than $\text{Proj}(B(x, d'), x)$) in region $B(x, d')$. In Fig. 3, an adversarial input found by this step, when starting the search from $x_2$, is $x_3$, which is also a vertex of $B(x_0, d_2)$.

On lines 9–12, we essentially check whether the search step was successful in finding another adversarial input $x''$. Recall that $\text{DS-Binary}$ and $\text{DS-Multiclass}$ only terminate when such an input is found, but in practice, we bound their number of iterations. If this bound is reached, they might not return an adversarial example. If they do, like input $x_3$ in Fig. 3, the algorithm iterates (line 13). If not, like when starting the search from input $x_4$ in the figure, which is a projection of $x_3$ on $B(x_0, d_1)$, then we return the projected input and terminate.

5. **EXPERIMENTAL EVALUATION**

In this section, we evaluate DeepSearch by using it to test the robustness of deep neural networks trained for popular datasets. We also compare its effectiveness with state-of-the-art black- and whitebox approaches. Our experiments are designed around the following research questions:

**RQ1:** Is DeepSearch more effective than random fuzzing?

**RQ2:** Is DeepSearch more effective than state-of-the-art techniques for finding adversarial examples?

**RQ3:** Is DeepSearch with iterative refinement effective in finding adversarial examples with low distortion rates?

**RQ4:** How does reducing the number of queries to the network under test affect the effectiveness of DeepSearch?

In Sect. 5.3, we present experimental results providing answers to these questions. Note that the fourth question uses the term ‘queries’ to refer to the number of times we evaluate classification function $f$, e.g., $2nk$ times in Algs. 1 and 2. Sects. 5.1 and 5.2 discuss our experimental setup and the metrics we use to evaluate and compare the effectiveness of our technique.

5.1 Evaluation Setup

**Datasets and network models.** We evaluate our approach on deep neural networks trained for two popular datasets, namely MNIST [42] and CIFAR-10 [37]. For MNIST, we trained a LeNet-5 [41] network with 99.2% test accuracy, and for CIFAR-10, a ResNet-32 [28] network with 92.19% test accuracy.

For each dataset, we first randomly selected 1100 images from the test set and carried out our experiments only on the images that were correctly classified by the networks we trained. For MNIST, 1085 images were correctly classified by the LeNet-5 network, and for CIFAR-10, 1024 images by the ResNet-32 network.

**Random fuzzing.** Random fuzzing is a very simple technique for testing the robustness of a neural network, and in practice, it can prove effective in finding adversarial examples. In the following, we introduce two random-fuzzing approaches that we use as baselines in our experiments.

**Basic random fuzzing** For $x \in \mathbb{R}^n$ and $d \in \mathbb{R}$, we generate 6000 images within $B(x, d)$ with random mutations.

**Algorithm 3: DeepSearch with iterative refinement.**

```
Input: $x \in \mathbb{R}^n$, adversarial input $x' \in B(x, d) (d \in \mathbb{R})$, function $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$
Output: an adversarial input $x'' \in B(x, d') (d' \leq d)$

 Function $\text{DS-Refinement}(x, x', f)$ is

1. repeat
2. $d := ||x - x'||_\infty$
3. apply bisect search to find the smallest distance $d' \leq d$ such that $\text{Proj}(B(x, d'), x')$ is an adversarial example
4. if $f$ is binary then
5. $x' := \text{DS-Binary}(x, \text{Proj}(B(x, d'), x'), f, d')$
6. else
7. $x' := \text{DS-Multiclass}(x, \text{Proj}(B(x, d'), x'), f, d')$
8. if $x''$ is an adversarial example then
9. $x' := x''$
10. else
11. $x' := \text{Proj}(B(x, d'), x')$
12. until $x'$ is not an adversarial example
13. return $x'$ and $d'$

```
Iterative random fuzzing. For $x \in \mathbb{R}^n$ and $d \in \mathbb{R}$, we perform iterative random fuzzing as follows.

1. Seed-pool initialization: We first generate 1000 images within $\mathcal{B}(x, d/5)$ with random mutations. From these, we select the 10 best images. In particular, for $f(x) > 0$ (resp. $f(x) < 0$), an image $x'$ is selected if $f(x')$ evaluates to one of the 10 smallest (resp. largest) values of $f$.

2. Iteration: For each image $x'$ in the pool, we generate 100 images within $\mathcal{B}(x', d/5) \cap \mathcal{B}(x, d)$ with random mutations. So, for all seed images, we derive a total of 1000 random images. From these, we then select the 10 best images and populate the pool with them for the next iteration. We iterate 9 times in our experiments.

Existing approaches. We compare DeepSearch with three state-of-the-art approaches for generating adversarial examples, which we describe below.

- The Fast Gradient Sign Method (FGSM) [24] is a popular whitebox technique, optimized for the $L_{\infty}$ distance metric. For an input $x$, it computes an adversarial example $x'$ as $x' = x + \epsilon \cdot \text{sign}(\nabla_x f(x, l))$, where $L_f(x, l)$ is the loss function, $f$ the classification function, and $l$ the label given to $x$ by $f$.

- The Basic Iterative Method (BIM) [39], also called iterative FGSM, extends FGSM with iterations. Starting from an image $x$, each iteration takes a small step $\alpha$ toward the gradient sign and clips the new image such that it is within $\mathcal{B}(x, \epsilon)$. An adversarial example is computed by $x'_0 = x$ and $x'_{i+1} = x'_i + \epsilon \cdot \text{clip}_[0, 1](\alpha \cdot \text{sign}(\nabla_x L_f(x, l)))$. In our experiments, we set $\alpha = 1$ and allow 120 (resp. 40) iterations for MNIST (resp. CIFAR-10).

- Gradient Estimation [5] is a blackbox technique that estimates gradients through queries to $f$. The effectiveness of single-step gradient estimation (sGE) is known to be comparable to FGSM. We use logits loss [5, 12] for sGE as it is more effective than cross-entropy loss [23] and set $\delta = 0.001$, where $\delta$ is a parameter that controls the estimation accuracy of this method.

Query reduction. Recall that for an $n$-dimensional input $x$, our technique makes $2n$ queries per iteration. To reduce this number, we adopt random grouping [5] to our setting:

1. We divide the $n$ dimensions into $\lceil \frac{n}{k} \rceil (0 < k \leq n)$ sets $G_1, \ldots, G_{\lceil \frac{n}{k} \rceil}$, where each set $G_i (1 \leq i \leq \lceil \frac{n}{k} \rceil)$ is derived by randomly selecting $k$ indices from $\{1, \ldots, n\} \setminus \cup_{j=1}^{i-1} G_j$. Note that there might only be $l < k$ remaining indices, in which case we select these.

2. For each set $G_i$, our technique mutates all coordinates that correspond to indices in the set toward the same direction at the same time. Hence, DeepSearch makes only 2 queries per set, namely $f(i_1/x_{i_1}, \ldots, i_l/x_{i_l})$ and $f(i_1/x_{i_1}, \ldots, i_l/x_{i_l})$, where $i_1, \ldots, i_l \in G_i$ and $l = |G_i|$. Consequently, the total number of queries per iteration reduces to $\lceil \frac{2n}{k} \rceil$. In our experiments, we show how random grouping affects the effectiveness of DeepSearch.

DeepSearch termination criteria. In our experiments, Alg. 2 terminates when $f(x_k)$ changes in the wrong direction 4 times.

Alg. 3 does not terminate as long as the current iteration decreases the normalized $L_{\infty}$ distance of adversarial examples by 0.001.

5.2 Metrics

To evaluate the effectiveness of DeepSearch, we use the following two metrics.

Misclassification rate. The misclassification rate measures the percentage of input images for which adversarial examples are found. The higher this rate, the more effective a given technique in finding adversarial examples. Assume we write $\text{findAdv}(x)$ to denote whether an adversarial example is found for input $x$. If so, we have that $\text{findAdv}(x) = 1$; otherwise, we have $\text{findAdv}(x) = 0$. For a set of images $X = \{x_1, \ldots, x_k\}$, the misclassification rate of a given technique is:

$$\text{MisR}(X) = \frac{1}{k} \sum_{i=1}^{k} \text{findAdv}(x_i)$$

Average distortion rate. Let sets $X = \{x_1, \ldots, x_k\}$ and $X_{adv} = \{x'_1, \ldots, x'_k\}$ be input images and adversarial examples, respectively. The average distortion rate between $X$ and $X_{adv}$ with respect to the $L_{\infty}$ distance is:

$$\text{AvgDR}_{L_{\infty}}(X, X_{adv}) = \frac{1}{k} \sum_{i=1}^{k} \frac{||x_i - x'_i||_{L_{\infty}}}{||x_i||_{L_{\infty}}}$$

As shown here, the lower this rate, the more subtle the adversarial examples. For approaches that achieve similar misclassification rates, we use this metric to determine which approach finds more subtle perturbations.

Other metrics. We do not measure time in our experiments; our aim is to show that our blackbox technique is more effective than state-of-the-art whitebox approaches. These approaches are typically fast due to their whitebox nature—they have access to more information about the network under test. So, comparing time would disadvantage DeepSearch.

For comparing iterative approaches, we do not bound the number of iterations to the same fixed value. This is because the notion of an iteration is inherently different across approaches. We, instead, use the same distance metric ($L_{\infty}$) for all approaches.

5.3 Experimental Results

In our experiments, we consider the following four variants of DeepSearch:

1. Single-step DeepSearch (sD) implements Alg. 2 but executes lines 7–9 only once.
2. Iterative DeepSearch (iD) implements Alg. 2 as is (using the termination criterion discussed in Sect. 5.1).
3. DeepSearch with single-step refinement (DsR) implements Alg. 3 but executes lines 3–12 only once.
4. DeepSearch with iterative refinement (DiR) implements Alg. 3 as is (using the termination criterion discussed in Sect. 5.1).

In the rest of this section, we use the following abbreviations and use both cross-entropy loss and logits loss for FGSM and BIM: bRF for basic random fuzzing, IRF for iterative random fuzzing,
FGSM-X (resp. FGSM-L) for FGSM with cross-entropy (resp. logits) loss, BIM-X (resp. BIM-L) for BIM with cross-entropy (resp. logits) loss.

**Results on misclassification rate.** Our experimental results on the misclassification rate of the different techniques are shown in Fig. 4.

Overall, DeepSearch is significantly more effective than the two random-fuzzing approaches (bRF and iRF). Observe that, for MNIST, random fuzzing is not as effective as for CIFAR-10. In fact, for CIFAR-10, random fuzzing is quite effective for a large $L_{\infty}$ distance. As shown in the figure, the misclassification rate of bRF (resp. iRF) surpasses the three single-step approaches (sGE, sD, and FGSM) when the distance is greater than 24 (resp. 16).

When comparing single-step approaches, we observe that **single-step DeepSearch is more effective than sGE and whitebox FGSM for both MNIST and CIFAR-10.** For the MNIST model, the advantage of sD is more prominent when the $L_{\infty}$ distance ranges from 0.15 to 0.4. For this distance range, the misclassification rate of sD is 10–20% higher than sGE and 15–28% higher than FGSM. For CIFAR-10, when the distance ranges from 4 to 16, the difference is again more noticeable. For this range, sD is 1–3% more effective than sGE and 4–7% more effective than FGSM. It is important to note here that sD is more effective than sGE while performing half of the queries to function $f$. Recall from Sect. 2.1 that, in practice, sD performs $n$ queries, whereas sGE requires $2n$.

When comparing iterative approaches, **iterative DeepSearch closely matches the effectiveness of whitebox BIM for both models.** For the MNIST model, when the $L_{\infty}$ distance is above 0.2, the misclassification rates of both iD and BIM are close to 100%. The results are similar for CIFAR-10 when the distance is above 4. Despite the comparable effectiveness of iD and BIM, DeepSearch with iterative refinement (DiR) achieves a lower distortion rate than BIM, as we discuss later in this section. We also mention our empirical observation that DeepSearch terminates in 3–4 iterations for the vast majority of input images (around 95%) for which DeepSearch finds adversarial examples.

For DeepSearch variants, we observe that iD is significantly more effective than sD. This confirms that the iterative version of DeepSearch (implemented in Alg. 2) is indeed effective in finding adversarial examples.

**Results on average distortion rate.** Our experimental results on the average distortion rate of the different techniques are shown in Fig. 5.

As shown in the figure, only DeepSearch with single-step and iterative refinement (DsR and DiR) as well as BIM with logits loss (BIM-L) are effective in finding subtle adversarial examples, even more so when the $L_{\infty}$ distance is large. For both MNIST and CIFAR-10, **DeepSearch with iterative refinement achieves the lowest average distortion rate.**

For both models, BIM-L achieves a lower distortion rate than DsR. However, DiR is even better than BIM-L. Specifically, for MNIST, when the $L_{\infty}$ distance is between 0.15 and 0.4, the distortion rate of DiR is 2–3% lower than BIM-L. For CIFAR-10, the distortion rates are similar but slightly better for DiR. Overall, **DeepSearch with iterative refinement is more effective in finding subtle adversarial examples than whitebox BIM.** This is a notable result given that DiR (or iD) also matches the misclassification rate of BIM-L despite its blackbox nature.

In comparison to iD, DsR reduces the distortion rate significantly. For MNIST, when the $L_{\infty}$ distance ranges from 0.15 to 0.4, DsR reduces the distortion rate by 3–22%. For the CIFAR-10 model and a distance range between 12 and 32, DsR reduces the distortion rate by 4–12%. These percentages are even higher for DiR. In particular, for MNIST, DiR reduces the distortion rate by 4–28%, and for CIFAR-10, by 5–13%. These results confirm the effectiveness of refinement (Alg. 3) in generating subtle adversarial examples.

**Results on query reduction for DeepSearch.** We now show how query reduction based on random grouping affects DeepSearch with iterative refinement (DiR). Figs. 6 and 7 show how different values of $k$ (see Sect. 5.1) impact the misclassification rate and average distortion rate of our technique. In our setting, $k$ may range from 1 to 256.

As shown in Fig. 6, as $k$ increases, the misclassification rate of DeepSearch decreases, and therefore, so does its effectiveness in finding adversarial examples. For example, for MNIST, when the $L_{\infty}$ distance is between 0.1 and 0.4, the misclassification rate drops by 32–85% as $k$ increases from 1 to 256. Similarly, for CIFAR-10, when the distance is between 4 to 32, the misclassification rate drops by 4–78%.

In Fig. 7, the average distortion rate of DeepSearch increases for larger values of $k$, and thus, its effectiveness in generating subtle
DeepSearch: Simple and Effective Blackbox Fuzzing of Deep Neural Networks

Figure 5: Comparison of average distortion rates.

Although the effectiveness of DeepSearch decreases as the value of $k$ increases, the number of queries may still be reduced without compromising the advantage of DeepSearch over, say, whitebox FGSM. For example, for MNIST, when the $L_{\infty}$ distance is from 0.25 to 0.4 and $k \leq 16$, DeepSearch still achieves a higher misclassification rate and a lower distortion rate than FGSM. The same holds for CIFAR-10 when the distance is from 16 to 32 and $k \leq 128$.

5.4 Threats to Validity

We have identified the following three threats to the validity of our experiments.

Datasets and network models. Our experimental results may not generalize to other datasets or network models. However, we used two of the most popular datasets for image classification, MNIST and CIFAR-10. Moreover, our network models have very high test accuracy, 99.2% for LeNet-5 and 92.19% for ResNet-32.

Existing approaches. The second threat is related to the choice of existing approaches with which we compare. DeepSearch uses iterative linearization of non-linear networks and is tailored to the $L_{\infty}$ distance metric. We, thus, compare with approaches that are similar in spirit.

Both FGSM and BIM perform linear perturbations of non-linear models and are optimized for the $L_{\infty}$ distance. DeepFool [50] also uses linearization of networks, but it is optimized for the $L_2$ distance, so we do not compare with it.

Blackbox gradient-estimation methods [5] are more effective than other query-based blackbox techniques. We selected sGE for comparison because it may be more effective than FGSM (see Fig. 4). On the other hand, we omitted iterative gradient estimation because, when step $\alpha$ (see Sect. 5.1) is sufficiently small, the effectiveness of the approach should be comparable to BIM, with which we compare.

Fairness of comparison. The selection of parameters for each approach could affect the fairness of our comparison.

The number of iterations of BIM and iterative DeepSearch are not comparable; each iteration performs fundamentally different computations. We chose a bound for BIM that is sufficiently large for adversarial examples to reach the edge of the neighborhood around the original image. We set $\alpha = 1$ as suggested by the authors of BIM.

In sGE, $\delta$ affects the precision of the gradient estimation. We set $\delta = 0.001$, which is much more precise than the value chosen by the authors of sGE ($\delta = 0.01$).
versarial examples in neural networks and used box-constrained based attack. The boundary attack used NES et al. phenomenon of transferability [53] and many blackbox attacks require a large number of queries.

DeepSearch neural networks. As a blackbox approach, that performs adversarial attacks through iterative linearization of it with iterative procedures. DeepFool generation of adversarial examples. BIM improved FGSM by extending it with iterative procedures. DeepFool is closer to FGSM, BIM and DeepFool. Goodfellow et al. [50] argued that the primary cause of adversarial examples is the linear nature of neural networks, and they proposed FGSM that allows fast generation of adversarial examples. BIM improved FGSM by extending it with iterative procedures. DeepFool is another method that performs adversarial attacks through iterative linearization of neural networks. As a blackbox approach, DeepSearch differs with FGSM, BIM and DeepFool in its way to perform iterative search.

Blackbox adversarial attacks are more difficult than whitebox ones, and many blackbox attacks require a large number of queries. Papernot et al. [53, 54] explored blackbox attacks based on the phenomenon of transferability [53, 68]. Chen et al. [13] and Bhagoji et al. [5] proposed blackbox attacks based on gradient estimation [40, 65]. Uesato et al. [71] used SPSA [64], and Ilyas et al. [32] used NES [59]. Narodytska et al. [51] performed a local-searched based attack. The boundary attack [6] only requires access to the final decision of neural networks. DeepSearch is closer to the work of Bhagoji et al. [5] (which approximates FGSM and BIM), but DeepSearch does not rely on gradient estimation.

Although research on developing adversarial attacks is moving fast, research on defending neural networks against adversarial attacks is relatively slow [1, 2, 9–12, 15, 20, 29, 46, 62]. Many defense techniques are shown to be ineffective soon after they have been developed. We refer to the work of Carlini et al. [8] for a more detailed discussion on evaluating adversarial robustness.

Testing deep neural networks. Recently, significant progress has been made on testing neural networks. Several useful test coverage criteria have been proposed to guide test case generation: DeepXplore [56] proposed neuron coverage and the first whitebox testing framework for neural networks; DeepGauge [47] proposed a set of finer-grained test coverage criteria; DeepCT [48] further proposed combinational test coverage for neural networks; Sun et al. [66] proposed coverage criteria inspired by MC/DC; Kim et al. [35] proposed surprise adequacy for deep learning systems. Sekhon et al. [60] and Li et al. [43] pointed out the limitation of existing structural coverage criteria for neural networks. Li et al. [60] also discussed improvements for better coverage criteria.


Liu et al. [44] classified recent work into five categories: Reachability-analysis based approaches include MaxSens [77], ExactReach [76], and AI² [21]; NSVerify [45], MIPVerify [70] and ILP [1] are based on primal optimization; Duality [18], ConvDual [75] and Certify [58] use dual optimization; Fast-Lin & Fast-Lip [75], ReluVal [72] and DLV [31] combine reachability with search; Sherlock [17], Reluplex [33], Planet [19] and BaB [7] combine search with optimization. Lie et al. [44] provide a more detailed comparison and discussion on the above mentioned work.

7 CONCLUSION

We proposed and implemented DeepSearch, a novel blackbox-fuzzing technique for testing deep neural networks. DeepSearch is simple and effective in finding adversarial examples with low distortion. To the best of our knowledge, DeepSearch is among the early approaches advancing blackbox fuzzing for neural networks.
REFERENCES


