FOX: Fooling with Explanations Privacy Protection with Adversarial Reactions in Social Media
Noreddine Belhadj-Cheikh, Abdessamad Imine, Michaël Rusinowitch

To cite this version:
Noreddine Belhadj-Cheikh, Abdessamad Imine, Michaël Rusinowitch. FOX: Fooling with Explanations Privacy Protection with Adversarial Reactions in Social Media. PST 2021 - 18th Annual International Conference on Privacy, Security and Trust, Dec 2021, Auckland/Virtual, New Zealand. hal-03480304

HAL Id: hal-03480304
https://inria.hal.science/hal-03480304
Submitted on 14 Dec 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
FOX: Fooling with Explanations
Privacy Protection with Adversarial Reactions in Social Media

Noreddine Belhadj-Cheikh, Abdessamad Imine and Michaël Rusinowitch
Lorraine University and Loria-Cnrs-Inria Nancy-Grand Est
Nancy, France
firstname.lastname@loria.fr

Abstract—Social media data has been mined over the years
to predict individual sensitive attributes such as political and
religious beliefs. Indeed, mining such data can improve the user
experience with personalization and freemium services. Still, it
can also be harmful and discriminative when used to make
critical decisions, such as employment. In this work, we investi-
gate social media privacy protection against attribute inference
attacks using machine learning explainability and adversarial
defense strategies. More precisely, we propose FOX (FOoling with
eXplanations), an adversarial attack framework to explain and
fool sensitive attribute inference models by generating effective
adversarial reactions. We evaluate the performance of FOX
with other SOTA baselines in a black-box setting by attacking
five gender attribute classifiers trained on Facebook pictures
reactions, specifically (i) comments generated by Facebook users
excluding the picture owner, and (ii) textual tags (i.e., alt-
text) generated by Facebook. Our experiments show that FOX
successfully fools (about 99.7% and 93.2% of the time) the
classifiers, outperforms the SOTA baselines and gives a good
transferability of adversarial features.

Index Terms—Social Networks, Privacy, Adversarial Machine
Learning, Explainability.

I. INTRODUCTION

Online Social Network (OSN) platforms have attracted
billions of users resulting in a massive amount of data. For
instance, every 60 seconds on Facebook: 510,000 comments
are posted, 293,000 statuses are updated, 4 million posts
are liked, and 136,000 photos are uploaded [20]. This large
amount of data jeopardizes individuals’ privacy due to its
richness of content, including users’ behavior, relationships,
reactions, and other private information. The risk can expand
up to the traceability and identification of users. Indeed, users
remain highly vulnerable to attribute inference attacks which
consist in gaining illegitimately private attributes (such as
gender or age) from publicly available data using classical or
deep learning models. This work focuses on attribute inference
attacks in OSNs and proposes a framework to mitigate the
risks inherent in such attacks.

Popular OSNs like Facebook, Instagram, and Twitter rely on
online advertising to be profitable and keep their services free
of charge. They enable advertisers to target potential clients
among billions of users. Users’ data is therefore considered as
an important asset to build effective and profitable ad targeting
platforms. In the meantime, OSNs often provide options for
users to control who can view their data, including profile
attributes and their activity on the platform. Nevertheless,
online advertising raises privacy and security concerns due
to misleading and contradicting privacy settings of some
OSNs [1], [4]. For example, Facebook enables users to define
explicitly which attributes, and interest categories can be used
by advertisers to target them. However, Facebook overrides the
user setting and targets users even through unwanted interests
(see Fig. 1).

Figure 1: A contradicting statement in one of Facebook’s privacy control
settings. Facebook states that this setting is intended to prevent advertisers
from targeting a user with an unwanted interest category (green), whereas
Facebook retains the right to target the user with the unwanted interest
category (red).

In addition to the deceitful privacy management in OSNs,
users became highly threatened by sensitive attribute inference
attacks due to the development of strong models (e.g., deep
learning models) that benefited from tremendous amounts of
user-generated data in social media platforms and the low cost
of computational power.

Although working directly on data generated by target users
is straightforward and practical, users can be more cautious
about their activity and the data they post to limit risks to
their privacy. In [15], the authors showed it is possible to
infer sensitive attributes even when the target user is discreet
about those attributes by mining reactions that the target
user received on their pictures (e.g., comments from friends).
Reactions come from other users and/or the OSN platform
(e.g., Facebook picture tagging and Reddit bots). Data received
from other users (e.g., friends) is less manageable than data

This work is partially supported by DIGITRUST http://lue.univ-lorraine.
fr/fr/article/digitrust/.
generated by users themselves. For instance, a user may avoid words that leak information about their gender. However, it is not practical to ask all users who react to their pictures to do the same. As a result, the threat of sensitive information leakage by the reactions of others is more critical.

Despite the performance of Deep Neural Networks (DNN), research efforts in adversarial attacks have shown that they are vulnerable to strategically crafted inputs, named adversarial examples \[5\]. In particular, adversarial attacks against images witness notable success. However, the advancement of adversarial attacks techniques in Computer Vision is not directly applicable to neural networks trained for Natural Language Processing (NLP), where the textual input space is discrete.

In an attempt to protect OSN users from attribute inference attacks on non-user generated data, we propose FOX (FOoling with eXplanations), a framework based on explainability tools (e.g., LIME \[19\]) that generates adversarial reactions to attack sensitive attributes black-box classifiers. A user who wants to protect their profile against attributes inference attacks may employ fake profiles or ask a list of trusted friends to add the reactions recommended by FOX. Fig 2 illustrates an attack performed by FOX.

We formally define the problem as follows. Let \(x\) be a publication with a set of reactions \(R\) that \(x\) received. Given \(x\) and \(R\), let \(h\) be the target classifier mapping \(x\) to some class \(c\). Our goal is to find the adversarial reactions \(R^{adv}\) which when appended to the original reactions \(R\) guarantees that \(h(x, R) \neq h(x, R \cup R^{adv})\). In addition to a successful attack, the generated adversarial reactions must also adhere to constraints corresponding to their textual nature (e.g., grammatical well-formedness) and be stealthy, thus undetected by adversarial attacks defense systems. Moreover, the protection framework should ensure adaptability to different target classifiers (e.g., Neural Architectures, Logistic Regression, and Ensembles).

Our main contributions in this work are as follows:

- To our best knowledge, we introduce the first method that prevents sensitive attribute inference attacks against OSN users by protecting their publications with adversarial reactions.
- For that, we develop a framework using LIME explanations to perform adversarial attacks. Our framework can fool multiple types of models, including neural models (e.g., DNN), classical models (e.g., logistic regression), and their stacking.
- As a real-world application, we have trained deep neural network classifiers for gender attribute inference on the following Facebook picture reactions: (i) comments posted by friends, friends of friends, or strangers, and (ii) textual tags (i.e., alt-texts) generated by Facebook to describe the content of pictures. Note that gender attribute is highly relevant for targeted advertising. Furthermore, to adhere to a realistic black-box setting without prior information about the classifier, we have to consider models with different architectures such as Recurrent Neural Networks (RNNs), Convolutional Neural Networks (CNNs), Attention-based, Ensembles, and logistic regression. Experimental results show that FOX is very effective.
- We further investigate the transferability of the extracted features for one model to attack another model. Experimental results demonstrate that FOX gives a good transferability of adversarial features.

This paper is organized as follows. In Section II we review the related works. Section III describes our framework FOX. We present our case study in Section IV and the experimental evaluation in Section V. Section VI draws limitations of our approach. We conclude with future works in Section VII.

II. RELATED WORK

A. Attribute Inference Attacks

A user’s profile may contain self-identifying attributes such as gender, hobbies, age, visited places, and political views. Social networks usually offer users the possibility to limit the visibility of their attributes as means of controlling their privacy (e.g., being visible to friends only). Therefore, the network is a mixture of users with private and public information. The attack’s goal is to infer the private or missing attribute of a user by leveraging publicly available data. The attacker could be the social network service provider itself, advertisers, criminals, and data brokers. Most works on attribute inference attacks belong to three groups: friend-based \[8\], behavior-based \[22\], or their combination \[7\]. In addition, there exist works that leverage other sources of information such as writing style, liked pages, and group subscriptions. Authors in \[16\] took a different approach where they utilize reactions (e.g., comments generated by friends and Facebook-generated alt-text) received on a target user-posted picture.

B. Attacking Profile Attribute Predictors

Several works study adversarial attacks that are specific to user-generated data, but very few consider attacks on profile attribute classifiers using reactions generated by other users. \[2\] brings into the problem of evasion and poisoning attacks on profile attributes inference models based on user’s Facebook liked pages. In evasion attacks, the user edits their profile information (Facebook liked pages) by adding or removing features (Liking/Unliking pages) that contribute to a particular attribute in order to interfere with the prediction of the target classifier. But, to succeed in poisoning attacks, \[2\] requires the manipulation of 1% of the training data to decrease the overall target classifier performance. Note that the training data is generally not accessible, especially for black-box models. In \[11\], the authors study a problem close to ours where the goal is to generate and add malicious comments to a news article causing a neural fake news detector to misclassify it as REAL/FAKE news. They propose MALCOM, a system comprising a Conditional Text Generator Module for comments generation and a Style Discriminator Module to preserve syntax and coherency between the article’s content and the generated
comments. Despite MALCOM’s good performance, one of the conditions for a black-box setting is violated when training the system and the target models with 100% overlapping data, which should not be the case in a realistic black-box setting. To respect this condition, we introduce a portion of non-overlapping data to train the target models. Unlike [2], [11], we attack the target classifiers with multiple reaction types (Comments and Facebook Alt-Text), which are not generated by the target user, and our attack is not limited to neural models only. Moreover, the authors of [11] do not provide detailed information about the system components nor release the code as they promised upon acceptance of their paper. Consequently, we were unable to implement and apply it to our case study for an accurate comparison.

C. Adversarial Text Generation

Generating text under an adversarial setting, i.e., to attack ML classifiers, is more challenging due to the discrete nature of the text [25]. Although there has been many efforts to construct adversarial samples to attack text-based ML models [10], [12], [13], most of them focus on making minimal modifications (e.g., addition, removal, or replacement,) in character [12], [13] or word level [10], [12] of a span of text, through either a set of predefined templates [12] or a search mechanism with constraints [10], [13]. Despite the success of these methods, they are only designed for attacking static features, such as altering the text of a review to fool a sentiment analysis classifier. They are not developed for dynamic sequential input like comments where content can be added over time. Moreover, these attack methods primarily require existing content and are not adapted to cases where the initial content alteration is not possible (e.g., a Facebook user cannot modify comments of others). Therefore, we propose a framework to generate adversarial reactions with strategies that can effectively attack static input (e.g., alt-text) and dynamic sequential inputs where the initial input should not be altered (e.g., comments).

III. FOOLING WITH EXPLANATIONS: FOX FRAMEWORK

We propose a robust framework which, given an initial dataset $X$ (e.g., Facebook pictures reactions) and an explainability tool (e.g., LIME), can extract strong adversarial features $E_{\text{strong}}$ from reactions. These features will be used to construct adversarial reactions to fool black-box classifiers and prevent them from threatening social media users’ privacy. In the following, we describe FOX framework, and all used notations are listed in Table I.

**Step 1 - Building strong features list:** FOX requires a dataset $X$ (e.g., a set of Facebook pictures with their reactions) to be collected. Each instance $x \in X$ admits a set of reactions $R_x$ (e.g., comments, alt-text, likes for a given picture) and each reaction $r \in R_x$ admits a set of features $F_r$ (e.g., words can be the features for a textual reaction such as comments). We assume that different reaction types admit disjoint sets of features. Therefore, we propose a framework to generate adversarial reactions with strategies that can effectively attack static input (e.g., alt-text) and dynamic sequential inputs where the initial input should not be altered (e.g., comments).

![Figure 2: An adversarial comment generated by FOX misleads a gender attribute classifier to predict a Male picture owner as Female.](image)
Table I: Notations

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X$</td>
<td>Dataset used for strong features extraction</td>
</tr>
<tr>
<td>$x$</td>
<td>Instance of a dataset (e.g., picture)</td>
</tr>
<tr>
<td>$x_{adv}$</td>
<td>Adversarial instance</td>
</tr>
<tr>
<td>$R_x$</td>
<td>Reactions set of $x$</td>
</tr>
<tr>
<td>$F_r$</td>
<td>Features set of reaction $r$</td>
</tr>
<tr>
<td>$h(.)$</td>
<td>Black-box classifier</td>
</tr>
<tr>
<td>$h_t(.)$</td>
<td>Class label returned by the black-box classifier</td>
</tr>
<tr>
<td>$E(.)$</td>
<td>Explainability tool</td>
</tr>
<tr>
<td>$\mathcal{E}$</td>
<td>Features set extracted from $X$ by $E(.)$</td>
</tr>
<tr>
<td>$\mathcal{E}_{strong}$</td>
<td>Features filtered from $\mathcal{E}$</td>
</tr>
<tr>
<td>$t$</td>
<td>Instance of $\mathcal{E}$. It is a tuple containing the value and contribution class denoted $\langle f, c \rangle$</td>
</tr>
<tr>
<td>$t_{mc}$</td>
<td>Most contributing feature</td>
</tr>
<tr>
<td>$\mathcal{P}$</td>
<td>Set of perturbed instances of $x$</td>
</tr>
<tr>
<td>$Y$</td>
<td>Set of classes</td>
</tr>
<tr>
<td>$y'$</td>
<td>Target class</td>
</tr>
<tr>
<td>$I$</td>
<td>Maximal number of iterations</td>
</tr>
<tr>
<td>$N$</td>
<td>Maximal number of features per iteration</td>
</tr>
<tr>
<td>$A$</td>
<td>Set of all selected features to perform an attack</td>
</tr>
<tr>
<td>$A'$</td>
<td>Remaining features for an attack</td>
</tr>
<tr>
<td>$A_{\text{subset}}$</td>
<td>Set of features used in an iteration</td>
</tr>
<tr>
<td>$A_{\text{comments}}$</td>
<td>Set of comments features</td>
</tr>
</tbody>
</table>

We do a further filtering of the features list $\mathcal{E}$ to obtain the strong features list $\mathcal{E}_{\text{strong}}$ as follows. Let $T$ be a sequence of elements of $\mathcal{E}$: $t_1, t_2, \ldots, t_s$. We define $z_T$ to be a crafted instance that contains $f_1, f_2, \ldots, f_s$ in this order (see Fig. 4 for crafted instances example), where $t_i = \langle f_i, c_i \rangle$. Function $h_t(z_T)$ computes the class label of $z_T$. Then,

$$\mathcal{E}_{\text{strong}} = \{ \langle f, c \rangle | c = h_t(z_{\langle f,c \rangle}), \langle f, c \rangle \in \mathcal{E} \}$$

Figure 4: Let $\mathcal{E} = \{(\text{Hello}, \text{Male}), (\text{Handsme}, \text{Female})\}$. Subfigures (a), (b), and (c) illustrate the crafted Facebook pictures, containing reactions constructed from the features tuples $\{t_1\}, \{t_2\},$ and $\{t_1, t_2, t_3\}$, respectively.

Step 2 - Poisoning the input: Once we have constructed $\mathcal{E}_{\text{strong}}$ we are ready to poison the input in order to fool $h$. As shown in Algorithm 1, we first get the most contributing feature $f_{mc}$ to the original label $y$ of $x$ using the explainability tool. Hence we have:

$$t_{mc} = \langle f_{mc}, y \rangle = G_1(E, x, y, h)$$

Then we check if $t_{mc}$ exists in $\mathcal{E}_{\text{strong}}$, otherwise we compute its most similar using a feature type-specific similarity function (e.g., for words, we may use cosine similarity of their embeddings computed by a language model). After having $t_{mc}$ we choose the adversarial features according to Equation (3) to construct $A$ where $y'$ is the target label,

$$A = \{ t | h_t(z_{t_{mc}, t}) = y', t \in \mathcal{E}_{\text{strong}} \}$$

For each iteration $i$ we compute $A_{\text{subset}}$ that contains the top $N$ features according to a scoring function $S(.)$. We then perturb $x$ by creating adversarial reactions $R^*$ from the features in $A_{\text{subset}}$ and concatenate it with the set of reactions $R$ of the original instance $x$ resulting in a set of perturbed instances $\mathcal{P}$. The concatenation and the perturb functions depend on the feature's reaction type and the original reactions of $x$. For instance, permuting a publication with a feature extracted from a textual reaction such as a comment differs from perturbing it with a feature extracted from an emotional reaction. Hence, these functions are engineered in accordance with the type of reactions and their generation constraints.
Algorithm 1: Fooling by adding adversarial reactions

FOX \( (x, E, E^{strong}, h, y', I, N, S) \)

**Input:** \( x \) instance to protect, \( E \) explainability tool, \( E^{strong} \) Feature tuples set, \( h \) classifier, \( y' \) target class, \( I \) maximum number of iterations, \( N \) maximum number of selected features for each iteration, \( S \) features scoring function

**Output:** \( x_{adv} \) adversarial instance

\[ t_{mc} \leftarrow G_1(E, x, h_l(x), h) \] // most contributing feature
\[ A \leftarrow \{t \mid h_l(z_{mc, t}) = y', t \in E^{strong}\} \] // adversarial features

if \( t_{mc} \notin E^{strong} \) then
\[ A' \leftarrow A ;\]
i \leftarrow 1;
while \( i \leq I \) and \( A' \neq \emptyset \) do
\[ A_{sub} \leftarrow \text{top}_N(S, A');\]
\[ A' \leftarrow A' \setminus A_{sub},\]
\[ P \leftarrow \text{perturb}(x, A_{sub});\]
\[ x_{adv} \leftarrow \arg\max_{p \in P} h(p)[y'];\]
if \( h_l(x_{adv}) = y' \) then
\[ \text{return } x_{adv}; \] // solution found
else
\[ \text{if } h(x_{adv})[y'] > h(x)[y'] \text{ then}\]
\[ x \leftarrow x_{adv}; \]
\[ A' \leftarrow A ;\]
end
i \leftarrow i + 1
end
return None;

and the same user cannot perform two types of emotional reactions for the same publication.\footnote{This constraint applies to Facebook publications where a Facebook user can either react with a Like, Love, Wow, Angry, Sad once only. In contrast, the Reddit platform does not have this constraint.}

After generating \( P \), we search for the instance \( p \in P \) with the maximal change towards \( y' \). If \( h \) classifies \( x_{adv} \) as \( y' \), we return it, and the protection is considered successful. Otherwise, if \( x_{adv} \) has a more significant confidence score of \( y' \) than \( x \), we set \( x \) to be \( x_{adv} \) to perturb it in the next iteration. It is possible that the current \( A_{sub} \) neither succeeds in changing the label to \( y' \) nor increases the confidence score of \( y' \). Thus, if \( A' \) is not empty and we did not reach the maximum number of iterations \( I \), then we repeat the process with the remaining features.

The stop conditions of FOX are determined by these cases:
1) successfully fooling the classifier, 2) reaching the maximum number of iterations \( I \) without success 3)- exhausting all adversarial features without success.

In the following section, we will demonstrate FOX efficacy to protect Facebook pictures from gender inference attacks against different classifiers in a black-box setting. Then, we will compare it with other SOTAs methods.

IV. CASE STUDY: PROTECTING FACEBOOK PICTURES

We have applied our adversarial approach to Facebook pictures and reactions they generate, namely (a) friends’ comments (b) picture’s alt-text, which is a textual description of the picture generated automatically by Facebook\footnote{For simplicity, gender labels here are limited to Male or Female.}. The objective is to protect a Facebook user against gender inference classifiers trained on their picture reactions. We evaluate FOX with four classifiers of different architectures that we trained on a labeled dataset detailed in the following. Note that in adversarial attack works, the attacker is the party performing the adversarial attack against a model. Whereas, in our case, we consider the attacker to be the party performing an attribute inference attack. Here we utilize adversarial strategies as a protection solution.

A. Dataset

Our experiments are performed on a dataset collected from Facebook by \cite{16}. It consists of 4509 user-profiles and their pictures. Since we are interested in protecting against gender inference attacks, we have filtered out all the user profiles missing the gender label from the dataset. We have removed non-English comments using a language detection tool \cite{15}. We chose to train on reactions that are not generated by the owners of the pictures: the comments given by their friends on their picture and the alt-text description of this picture. We utilized weighted random oversampling to balance the number of pictures of female and male classes; The number of comments in a picture is considered the weight. The resulting preprocessed dataset statistics are shown in Table \ref{tab:gender_dataset_stats}.

<table>
<thead>
<tr>
<th>#pictures</th>
<th>#comments</th>
<th>#male</th>
<th>#female</th>
</tr>
</thead>
<tbody>
<tr>
<td>42,706</td>
<td>194,686</td>
<td>21,353</td>
<td>21,353</td>
</tr>
</tbody>
</table>

\( 2^{nd} \) column are limited to Male or Female.

To adhere to a realistic blackbox attack setting, we paid special attention to the data splitting. We first split the data into 60:40, overlapping and non-overlapping sets, respectively. Then we split the non-overlapping data into 4 chunks. Then for each target classifier, we assign 1 chunk of the non-overlapping data + overlapping set. With this splitting, we can ensure that at least 10% of the training data is unique for each classifier. Then for each classifier’s data we split it into train:validation:test:explainability.

The core component of FOX is the explainability tool. For this case study, we chose LIME \( (\text{Local Interpretable Model-Agnostic Explanations}) \)\footnote{https://github.com/marcotcr/lime} due to its prevalent adoption for interpreting blackbox models \cite{21, 23} and for being model-agnostic. We further adapted LIME to interpret inputs in...
the case of multiple reaction types since we are using two different reactions (comments and alt-text of type textual data, tags, respectively). (we will release the adaptation code)

FOX also requires a scoring function \( S(t) \) to obtain the \( \text{top}_N \) to be included in \( \mathcal{A}_\text{subset} \). We define \( S(t) \) as follows:

\[
S(t) = h(t_{mc}, t)[y^\prime],
\]

(4)

This scoring function measures the impact of injecting \( t \) with \( t_{mc} \) on the probability to have \( y^\prime \). Let \( t_{mc} \) be the most contributing feature. The \( \text{top}_N \) features are the ones that introduce the largest change towards \( y^\prime \) in the presence of \( t_{mc} \).

B. Adversarial Reactions Generation

To generate perturbed instances, we have defined the perturbation strategies for each reaction type under the constraints of being well-formed and stealthy. We have introduced several strategies in order to confuse the attacker:

1) Alt-text generation strategies: Facebook has designed and deployed automatic alt-text, which is a system to identify faces, objects, and themes from photos by applying computer vision technology. This system intends to help blind people get a clue of the content they are engaging with and to feel more connected and involved in Facebook. The alt-text generates a summary of the existing content for the image automatically. The technology can recognize a list of 97 concepts (tags), including people (e.g., people count, child, baby), objects (e.g., basketball, building, tree, cloud, food), settings (e.g., inside restaurant, outdoor, nature) and themes (e.g., close-up, selfie, drawing). The generated alt-text has a defined format described in [24]. Therefore, generating an adversarial reaction from alt-text should adhere to the following constraints: 1) order constraints. For example, people tags should come before themes tags 2) coherency constraints. For instance, "person" and "people" tags cannot co-exist. 3) a word that is not a tag is added in the form of a text. For instance, the word "pregnant" is not a tag; thus, injecting it would result in the alt-text: text that says "pregnant".

2) Comments generation strategies: we have defined three strategies for adversarial comments generation described below

- Single-Word-Comment: After analyzing the length of comments in the dataset, we have found that 12% are single-word comments (e.g., Beautiful, Wow, yes, etc.). The strategy of introducing single-word comments is interesting as it gives the lowest edit-distance compared to Word-Combination and Comment-Extraction strategies. We create a set of comment features that can be applied to generate a single-word comment. At each iteration, we check if the current single-word comment doesn’t make sense, we add punctuation (e.g., "!", "?"). For example, the comment "bro" alone may not make sense, but adding an interrogation mark (e.g., "bro?") makes it a plausible comment reaction.

- Word-Combination: In the word-combination strategy, we first define the length of the desired combinations \( l \), then we construct sentences of \( l \) comment features retrieved from the \( \text{ADV}_{\text{subset}} \) features set. We check the validity of the sentence using two tools: LanguageTool [15] for grammatical errors and the T5 model trained on (The Corpus of Linguistic Acceptability (CoLA)) [17] for linguistic acceptance.

- Comment-Extraction: Given the comment containing the most contributing word obtained in the Explainability step, we need to design a comment extraction and generation mechanism with word replacement. A suitable generated comment needs to fulfill the following criteria: (1) have a meaning similar to the fragment of the original comment used for generation (2) grammaticality of the generated comment should be preserved. In order to perform extraction and the selection of replacement words that meet such criteria, we propose the following workflow:

  - Clause Extraction: In this strategy, we perform word replacement only on a portion of the original comment. Specifically, only the clause/sentence containing the most contributing word is selected. First, we split the comment into sentences with (NLTK sentence tokenizer). Then we select the sentence containing the most contributing word and split it into clauses utilizing (benefact sentence parser). Finally, the clause \( C \) that has the most contributing word is selected for word replacement.

  - Replacement words sets construction: We randomly select from the extracted clause/sentence \( C \) the portion \( \sigma \) of words \( W \) to be replaced. We construct a set for all possible replacements of the selected word \( w_i \in W \). The replacement words set is initiated with the \( N \) closest words according to the cosine similarity between \( w_i \) and every other word in the adversarial comments features set. In the replacement words set of \( w_i \), we only retain those having an identical part-of-speech (POS) with \( w_i \) to ensure that the generated comment’s grammar is primarily maintained.

  - Comment Generation: For each \( w \in W \), we construct a set of sentences \( C' \) by substituting \( w \) in sentence \( C \) with a word from its replacement words set. We also compute the sentence semantic similarity between the source \( C \) and the resulting set of \( C' \). Concretely, we use Sentence Transformer Encoder to encode the two sentences into high dimensional vectors and use their cosine similarity score to approximate their semantic similarity. We set the similarity score threshold to 0.9. The sentence corresponding to the threshold will be considered to be the new source \( C \) for the subsequent word replacements. After iterating over all the words to replace \( w_i \in W \), we concatenate the resulting \( C \) with the set of comments of \( X \) to create an adversarial instance \( X_{adv} \). For an example, see Fig.

C. Target Classifiers

In this section, we describe the target classifiers used for FOX evaluation and comparison with the other SOTAs techniques. As we assume a blackbox setting, we have no information about the underlying architecture. Therefore we
have trained classifiers with various architectures (RNN, CNN, Attention, LR) and different encoding for the reactions. All the classifiers were trained on the first 100 comments of each picture and the alt-text. The best performance achieved by the trained classifiers is 0.74 in the F1 score. Table III summarizes the classifiers performance.

- **BERT**: We fine-tuned BERT [5] on the task of gender inference from the picture comments. We then used the mean of the fine-tuned model’s predictions over the set of comments to compute their final representation. Then we encoded the alt-text to a feature vector of $\mathbb{R}^{1024}$ using *distilbert-base-nli-stsb-mean* sentence embedding [18]. The set of comments vectors is then fed to three CNN layers with kernel sizes of (3, 1024), (3, 1024), (2, 1024); the output of each layer is max pooled, and the resulting pooled output of the three layers is concatenated then fed to a fully connected layer to compute the final representation of the comments. The alt-text embedding is fed to a fully connected layer to compute its final representation. Both final representations (comments and alt-text) are concatenated and fed to an FCN layer to infer the gender.

- **Roberta-CNN**: In this classifier, the picture comments and alt-text were encoded to a feature vector of $\mathbb{R}^{1024}$ using *Roberta-large-nli-stsb-mean* sentence embedding [18]. The set of comments vectors is then fed to three CNN layers with kernel sizes of (3, 1024), (3, 1024), (2, 1024); the output of each layer is max pooled, and the resulting pooled output of the three layers is concatenated then fed to a fully connected layer to compute the final representation of the comments. The alt-text embedding is fed to a fully connected layer to compute its final representation. Both final representations (comments and alt-text) are concatenated and fed to an FCN layer to infer the gender.

- **Distilbert-RNN**: In Distilbert-RNN, LSTM [9] layers are used to model the sequential dependency among comments. First, picture comments and alt-text were encoded to a feature vector of $\mathbb{R}^{768}$ each using *distilbert-base-nli-stsb-mean-token* sentence embedding [18]. To classify a picture, we feed the set of comments embeddings to the LSTM layers. Then we take the last hidden states computed for each LSTM layer and feed them to a fully connected layer to compute the final representation of the picture’s comments. The alt-text embedding is fed to a fully connected layer to compute its final representation. Then both final representations are concatenated and fed to an FCN layer for classification.

- **Pijani et al. [16]**: The authors employed several features extraction techniques to obtain relevant features to male and female classes then used them to train several classifiers specified in [15]. The authors have provided us with the code for training and evaluating their classifier.

- **Stacking**: For Stacking, we combine the predictions of all the models by performing hard voting on the predicted classes. The resulting prediction is the class with the majority of votes.

<table>
<thead>
<tr>
<th>Classifier</th>
<th>Accuracy</th>
<th>F1</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT</td>
<td>0.74</td>
<td>0.74</td>
</tr>
<tr>
<td>Stacking</td>
<td>0.73</td>
<td>0.73</td>
</tr>
<tr>
<td>Roberta-CNN</td>
<td>0.73</td>
<td>0.73</td>
</tr>
<tr>
<td>Distilbert-RNN</td>
<td>0.71</td>
<td>0.71</td>
</tr>
<tr>
<td>Pijani et al.</td>
<td>0.66</td>
<td>0.66</td>
</tr>
</tbody>
</table>

Table III: Target Gender Attribute Classifiers Performance

**D. Comparison of Attack Methods**

In this section, we will describe representative and SOTA adversarial text generators that we compared with FOX. Note that these attack methods require an initial text to attack. Therefore, we create a copy of the most contributing comment as an initial text, then concatenate it to the set of original comments of the picture and constrain the attack on the added comment only.
**TextFooler** [10]: This method identifies the most important words in the input and replaces them with semantically similar and grammatically correct words until it achieves the goal and fools the text classifier. This attack requires an initial text to attack.

**TextBugger** [12]: This method aims at fooling text classifiers by carefully introducing misspellings in a text which they call bugs. The bugs are created with the following strategies insert, delete, swap, substitute-c, substitute-w. They call bugs. The bugs are created with the following strategies insert, delete, swap, substitute-c, substitute-w. The bugs are created with the following strategies insert, delete, swap, substitute-c, substitute-w.

**DeepWordBug** [13]: This method searches for the highest-ranked tokens in a text using a scoring function defined in [13] and introduces simple character level perturbations to them to fool the classifier with a minimal edit-distance of the perturbation.

### V. Experimental Results

#### A. Attack performance

We quantify the effectiveness of the attack with the Attack Success Rate (ASR). For instance, an attack on $h$ with an ASR score of 90% indicates that an attacker can fool $h$ to predict an incorrect gender 90% of the time on all users publications that $h$ should have otherwise predicted correctly. All the experiments related to FOX have been performed with an iteration limit of $I = 20$ and a number of features per iteration of $N = 10$. For SOTA methods, we utilized the default parameters and their implementations in the TextAttack framework [14]. Table IV presents the evaluation of the Attack Success Rate (ASR) of all attack methods on the test data under a black-box setting. We can observe that FOX is able to achieve a near-perfect attack success rate attacking different classifiers, with the ASR ranging from 93% up to 99%. FOX/alt-text (FOX without alt-text strategies) directly compares to the other attacks since they attack only with comments. Despite employing only adversarial comments strategies with FOX, our method still outperforms other methods and is the only one to attack Pijani et al. [16] effectively. Whereas for the other attacks, the ASR is very low, ranging from 0.5% to 18% when attacking Pijani et al. [16].

#### B. Extracted features transferability

This section investigates the transferability of the extracted features for one model to attack another model. We observe that the extracted features are highly transferable from one model towards all the models in our experiments, with a minimum ASR of 80% and a perfect ASR of 100%. Results of transferability experiments are shown in Table IV.

#### C. Ablation study

In this section, we experiment FOX with different settings (number of features of the $\mathcal{E}_{strong}$, enable/disable adversarial reactions generation strategies) and study their impact on the ASR.

---

**a) $\mathcal{E}_{strong}$-related experiments:** We observe that the fewer features considered, the lower the attack success rate. The best attack success rate was achieved when considering all of the features in $\mathcal{E}_{strong}$ shown in Table VI with a slight decrease when considering 75% of the features. When limiting to only 25%, The ASR went even lower but still within an acceptable ASR within the range of 82%, 98% for BERT, Roberta-CNN respectively.

**b) Adversarial Reactions Generation Strategies-Related Experiments:** We show the impact of disabling one or a set of adversarial reaction generation strategies on the ASR with the following experiments.

- **Disable-comments ($d-c$)**: In this experiment, we consider only adversarial alt-text generation strategies. We noticed that the ASR decreased slightly for Roberta-CNN and DistilBert-RNN classifiers, whereas for BERT, it was nearly impossible to attack without adversarial comments generation strategies. Pijani et al. [16] had the second-highest decrease in ASR.

- **Disable-alt-text ($d-a$)**: In this experiment, we consider only adversarial comment generation strategies. The ASR decreased considerably for Roberta-CNN and BERT. The ASR had a slight decrease for Pijani et al. [16] classifier, whereas Distilbert-RNN was successfully attacked with a high ASR using only adversarial comments generation strategies.

### VI. Discussion

FOX comments generation is rule-based, and the definition of our generation strategies requires an expert in the used language. For instance, Chinese is written without spaces, unlike English (and other alphabetic writing systems), so defining the Comment-Extraction strategy requires understanding the language. Our usage of a rule-based approach is motivated by the fact that English grammar is well defined, which omits the need to train a generative language model, thus requiring a large amount of data. Moreover, we showed that we achieved the best ASR with a small amount of data with this approach. The notorious complexity of context extraction social networks data is due to the noisy nature of data in social networks and the diverse contexts that arise when users’ reactions (e.g., comments) shift from the original context of the publication [6]. Therefore, In our approach, we do not consider the context constraint when generating comments. Unlike GAN-based approaches, our method does not require a large dataset to build $\mathcal{E}_{strong}$ to create adversarial reactions for data mining models. Unlike previous works in adversarial text generation techniques. We employ an explainability tool to benefit from the model’s interpretability research. While the compared adversarial text approaches have successfully attacked static inputs (e.g., reviews), they performed weakly in dynamic inputs such as comments. In comparison, the performance experiments show that our approach has a high success rate and can attack various classifiers. Moreover, the techniques that relied on words substitution with synonyms failed to attack Pijani et al. [16]. In this classifier, out-of-vocabulary words (OOV) are replaced by similar ones from their vocabulary. This way of dealing with OOV words prevents techniques.
Table IV: Attack Performance on Different Attack Strategies and Target Classifier Architectures.

<table>
<thead>
<tr>
<th>Attack / Classifier</th>
<th>BERT</th>
<th>Distilbert-RNN</th>
<th>Roberta-CNN</th>
<th>Pijani et al.</th>
<th>Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>TextFooler</td>
<td>0.440</td>
<td>0.407</td>
<td>0.380</td>
<td>0.189</td>
<td>0.369</td>
</tr>
<tr>
<td>TextBugger</td>
<td>0.384</td>
<td>0.402</td>
<td>0.344</td>
<td>0.109</td>
<td>0.330</td>
</tr>
<tr>
<td>DeepWordBug</td>
<td>0.299</td>
<td>0.403</td>
<td>0.262</td>
<td>0.055</td>
<td>0.252</td>
</tr>
<tr>
<td>FOX / all-text</td>
<td>0.619</td>
<td>0.979</td>
<td>0.769</td>
<td>0.931</td>
<td>0.895</td>
</tr>
<tr>
<td>FOX</td>
<td>0.938</td>
<td>0.995</td>
<td>0.997</td>
<td>0.957</td>
<td>0.932</td>
</tr>
</tbody>
</table>

Table V: Strong features transferability across models for gender protection. The $i$th row represents the features extracted by the corresponding model, and the $j$th column represents the model attacked by these features. cell$_{i,j}$ represents the ASR of attacking the model $j$ using features extracted through the model $i$.

<table>
<thead>
<tr>
<th>Features / Classifier</th>
<th>BERT</th>
<th>Distilbert-RNN</th>
<th>Roberta-CNN</th>
<th>Pijani et al.</th>
<th>Stacking</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT</td>
<td>-</td>
<td>0.8</td>
<td>0.964</td>
<td>0.943</td>
<td>0.853</td>
</tr>
<tr>
<td>Distilbert-RNN</td>
<td>0.974</td>
<td>-</td>
<td>0.992</td>
<td>0.949</td>
<td>0.855</td>
</tr>
<tr>
<td>Roberta-CNN</td>
<td>0.971</td>
<td>1.0</td>
<td>-</td>
<td>0.952</td>
<td>0.848</td>
</tr>
<tr>
<td>Pijani et al.</td>
<td>0.917</td>
<td>0.8</td>
<td>0.952</td>
<td>-</td>
<td>0.823</td>
</tr>
<tr>
<td>Stacking</td>
<td>0.974</td>
<td>0.8</td>
<td>0.969</td>
<td>0.951</td>
<td>-</td>
</tr>
</tbody>
</table>

(а) $\mathcal{E}_{\text{strong}}$-related experiments  
(b) Adversarial Reactions Generation Strategies Experiments

Figure 6: FOX ablation study aimed to show the impact of different settings on the attack success rate (ASR) against the target classifiers.

<table>
<thead>
<tr>
<th>Models</th>
<th>Number of features</th>
</tr>
</thead>
<tbody>
<tr>
<td>BERT</td>
<td>375</td>
</tr>
<tr>
<td>Pijani et al.</td>
<td>637</td>
</tr>
<tr>
<td>Roberta-CNN</td>
<td>821</td>
</tr>
<tr>
<td>Distilbert-RNN</td>
<td>1291</td>
</tr>
<tr>
<td>Stacking</td>
<td>1295</td>
</tr>
</tbody>
</table>

Table VI: The number of extracted features of each target classifier that rely on substitutions with synonyms to destabilize the classifier’s predictions. In contrast, FOX extracted features that successfully fooled this class of classifier after an average of 3 iterations only. In the transferability experiments, we have shown that the extracted features for one model can be used to attack other models with a high success rate.

VII. CONCLUSION AND FUTURE WORK

We have proposed FOX, an adversarial attack framework for black-box models, that incorporates an explainability tool to generate effective adversarial reactions aimed at fooling different types of privacy threatening classifiers with a success rate of up to 100%. As a case study, we have applied FOX to protect the gender of Facebook users through adversarial reactions generated by our method. Furthermore, we have shown that FOX is more efficient than the other baselines and yields strong features with high transferability among classifiers even when the models have been trained with 10% of non-overlapping data. Our method allows for collaborative privacy protection in such a way the target user can be protected via the adversarial reactions posted by his/her trusted friends. Although based on black-box classifiers, our method can be extended to a white-box setting using only a white-box explainability tool.

As future work, we plan to apply FOX (i) on different data types (e.g., images) that may leak private information and (ii) to other types of online communities (e.g., question-and-answer websites like Quora, online discussions like Reddit) where users’ privacy could be highly threatened.

REFERENCES


