More Than Accuracy: Towards Trustworthy Machine Learning Interfaces for Object Recognition

Hendrik Heuer, Andreas Breiter
University of Bremen, Institute for Information Management, Germany
hheuer@ifib.de, abreiter@ifib.de

ABSTRACT
This paper investigates the user experience of visualizations of a machine learning (ML) system that recognizes objects in images. This is important since even good systems can fail in unexpected ways as misclassifications on photo-sharing websites showed. In our study, we exposed users with a background in ML to three visualizations of three systems with different levels of accuracy. In interviews, we explored how the visualization helped users assess the accuracy of systems in use and how the visualization and the accuracy of the system affected trust and reliance. We found that participants do not only focus on accuracy when assessing ML systems. They also take the perceived plausibility and severity of misclassification into account and prefer seeing the probability of predictions. Semantically plausible errors are judged as less severe than errors that are implausible, which means that system accuracy could be communicated through the types of errors.

KEYWORDS
User Experience; Human-Centered Machine Learning; Algorithmic Experience; Algorithmic Bias; Trust;

1 INTRODUCTION
Machine learning (ML) systems are designed to help users manage their photo collections, provide image captions for blind and visually impaired people, and enable self-driving cars to detect traffic signs and pedestrians [4, 24, 34, 40]. An HCI perspective on how to expose such ML systems that learn from data to users is only emerging [8, 16, 19, 39, 43]. In this paper, we explore what visualizations need in order to be perceived as transparent and trustworthy, which visualizations support the users in assessing the performance of object recognition systems and how different visualizations influence a user’s trust. Our goal is to examine the user experience of simple visualizations and their influence on trust. Trust is an important way to cope with risk, complexity, and a lack of system understanding [23]. Since ML systems can be complex, hard to understand and prone to fail at unexpected times, it is important to understand what makes peoples trust such systems. While a large body of research is already focused on developing complex visualizations of machine learning systems [31, 35, 38, 44], a thorough investigation of the user experience of ML systems in use is missing. In this paper, we examine how expert users assess the performance of a system based on the output of the system itself. ML systems often do not have dedicated interfaces. Users are usually just presented with the output of an ML system, often without any indication that they are interacting with an ML system. In this study, we contribute to the understanding of the user experience needs of such ML systems.

We want to support users with a basic understanding of machine learning systems in assessing a system in use. We investigated the visualizations and systems with experts from two groups: students who took an ML class, and engineers who develop ML systems. The participants in our study interacted with an object recognition system that labels images into ten different categories. Participants reviewed ten predictions for each of the 3x3 combinations of visualizations and machine learning systems. The ML systems achieve different accuracy, the visualizations differ in their complexity and in how much of an ML system they expose. After the participants rated the systems, we interviewed them about their experience. We answer the following research questions:

• Which of the visualizations help users with a background in ML assess the performance of ML systems? (RQ1)
• What makes a visualization helpful for the assessment of ML systems? (RQ2)
• How do the visualization and the accuracy of an ML system affect users’ trust and reliance? (RQ3)

2 RELATED WORK
The prevalence of complex, opaque, and invisible algorithms that learn from experience and data motivated a variety of investigations of algorithm awareness and algorithmic bias [9, 15]. Algorithmic bias, whether unintentional or intentional, was found to severely limit the perceived performance of an ML system. This motivated us to explore whether participants can assess the accuracy of an object recognition system in use, i.e. based on the system’s predictions. Our goal is to develop interfaces that support users in assessing the accuracy of an object recognition system in use.

To support trust in ML systems, we investigated different interfaces that displayed visualizations. Visualizations are a common way of communicating algorithmic processes [13, 19, 39]. A good visualization communicates complex ideas with clarity, precision, and efficiency [41]. We extend on prior work on how end-users interact with machine learning systems [3, 19, 39]. The research question about the helpfulness of visualization in assessing the accuracy of an ML system in use connects to Rader et al., who explored different explanation styles to communicate the news curation system on Facebook. They showed that explanations can help users determine whether a system is biased [30]. We focus on the user experience of simple visualizations and whether users can assess the accuracy of an ML system based on its output. Examples for visualizations of neural networks include showing the decision function [36], visualizing the filters [37] or providing explanations [32]. Such visualizations are highly specialized and presented without an empirical basis for their helpfulness [31, 35, 38, 44]. The large majority of ML papers does not evaluate their visualizations in user tests and does not compare their visualizations to basic visualizations [29, 32].

In this paper, we focus on trust in intelligent systems [17, 42] and automation [21, 27, 28] in the context of object recognition.
This context poses many risks that range from a cluttered photo collection to blind people becoming misinformed and self-driving cars hurting people. These risks directly connect to the complexity of deep neural networks, which are employed for many tasks. Even ML experts cannot fully understand or explain how and why deep neural networks make individual decisions. Since a full understanding is not possible, trust is important. This connects to prior work by Lee and See, who show that whether a task like deleting spam email is delegated depends on the trust in a system [21]. They state that trust guides reliance when the complexity of the automation makes a complete understanding impractical, which directly relates to the black box scenario in machine learning. Prior work by Muir [27], who modeled trust in a machine based on interpersonal trust, showed that users can meaningfully rate their trust in intelligent systems. Cramer et al. adopted Muir’s definition in the context of spam filters and showed that awareness and understanding seriously impact the users’ attitudes and behavior [6].

### 3 METHOD

For this study, we interviewed expert users after they reviewed ML-based object recognition systems. In a within-subject study, each participant rated 3x3 combinations of visualizations and machine learning systems via a web application. The ML systems had different levels of accuracy on an unseen test set. Participants were shown one image and one visualization at a time. After a waiting period of five seconds, participants also classified each of the images themselves. The waiting period was added to force participants to look at each image and each prediction carefully and keep them from clicking without looking. The order of the images was randomized but the same for each participant.

The study was conducted with machine learning systems trained to classify images based on objects. The ML systems were trained on the CIFAR-10 dataset, which consists of 60,000 32x32 color images and the ten classes: airplane, bird, car, cat, deer, dog, frog, horse, ship, and truck [20]. The CIFAR-10 dataset provides a task that is realistic, of limited scope (only ten classes), and so unique that none of the participants had prior experience in analyzing the output of such a system [12, 22, 26]. To compare systems with different levels of accuracy, we trained three nine-layer convolutional neural networks for two, ten and 160 epochs. We refer to the three systems we trained as Bad, Medium, and Good. The names are based on how many errors the systems make on average. The Bad system was trained for two epochs and has an accuracy of 51% (for the unseen testing data). The Medium system was trained for ten epochs and reached an accuracy of 65%. The Good system was trained for 160 epochs and achieved an accuracy of 83%. Training three neural networks with different levels of accuracy is challenging since the accuracy of an ML system does not improve linearly.

Participants were presented with the three visualizations shown in Figure 2: Top-1, Top-3, and Prob-3. The Top-1 visualization shows the prediction with the highest probability. This visualization was selected because it minimizes complexity and cognitive load by giving a simple, action-oriented answer to the classification task. It is the most commonly used interface for object recognition systems like Google Photos and Flickr [1, 18]. Top-3 shows the top three predictions ranked by their probability. We hypothesized that Top-3 would allow participants to make a more informed decision about the ML system since participants can use the ranking to compare the predictions. Prob-3 shows the same ranking and visualizes the probability of each prediction using a bar. The probabilities are based on the activation of the softmax unit of the convolutional neural network, which represents the probability distribution over ten different classes [11]. A high activation of a particular neuron indicates a high probability that this particular class is the correct classification of the image. Prob-3 was selected since it visualizes the probability distribution computed by the machine learning system, thus exposing that such ML systems operate in the regime of probabilities and correlations.

We investigate which visualizations help users with a background in ML to assess the performance of ML systems. We want to support people in assessing the trustworthiness of systems in use. Therefore, we conducted our investigation with a sample of experts that had sufficient knowledge of ML. We recruited our experts from two groups: ML students and ML engineers. Fifteen ML students (13 male, two female) were recruited at a large campus university in Germany. All students had attended a machine learning or data science course. The five ML engineers (all male) were recruited from a German augmented reality company with an ML focus. The study and the interviews were conducted in German and translated into English before the coding. Formed by prior work that focused on extreme users to gain rich insights into specific issues like customization in communication apps [5, 7, 14], we conducted an investigation with ML experts and students. This serves two purposes: (1) it allows us to investigate the needs that experts have when evaluating ML interfaces for object recognition, and (2), by extension, it allows us to understand how ML-based interface for photo-sharing websites or tools to manage photo collections need to be designed for end-users without a background in ML.

In the interviews, we elicited how the participants assess the accuracy of the ML systems and what information they believe they need for the assessment. We interviewed 15 participants (13
male, two female), who all had used the 3x3 combinations of visualizations and ML systems before the interview. Of the 15 interviewees, ten were students and five were engineers. We will cite statements by the interviewees as follows: If the fifth student made a statement, we indicate this as S5, while the third engineer is cited as E3. The interviews were audio-recorded and transcribed. In the semi-structured interviews, participants were asked how they determined the accuracy of a system, which visualization they found most helpful, and which visualization they found least helpful. We also asked participants to provide reasons for their answers. In addition to that, participants were asked whether they distinguished between “rellying on the prediction of the system” and “trust in the system”, which was followed by the question “If so, what was the difference for you?” This question was motivated by trust definitions that equal trust to reliance [21, 33]. Finally, participants were asked the open question: “What does trust mean to you in terms of machine learning?”. We coded the qualitative data using an inductive approach, where we read the raw data in detail and clustered textual quotations to identify emergent themes [25]. The material was analyzed step-by-step, assigning codes to individual words and sentences. After that, the material was revisited based on the codes that emerged. All codes were collected, sorted, and then combined into inductive categories. These analytical units were then sorted by the number of codes in the category and combined into inductive categories with a higher level of abstraction, merging semantically similar categories.

4 RESULTS

The first research question was which visualizations help users assess the performance of ML systems. We asked participants to name the most and the least helpful visualization. Of the three visualizations, all participants considered Prob-3 to be the most helpful visualization. Top-1 and Top-3 were never mentioned as the most helpful visualization. Top-1 was considered the least helpful visualization by the majority (66%) of people: three engineers and seven students named it in the interviews. Five participants (three students, two engineers) considered Top-3 to be the least helpful, though one participant also said that he found none of the visualizations helpful to assess the accuracy of the systems [E1].

Next, we investigated what makes a visualization helpful for this assessment (RQ2). For this, we explored the criteria and strategies that the participants apply to assess the ML visualizations. We found that participants want visualizations to expose the inner mechanics of the system [S2]. They highlighted the importance of more information [S4, S5], which allowed them to rely on the system to produce accurate results [S5] or since any information helps [E4]. One participant stated that the Prob-3 visualization showed that the system does not have a crystal ball that tells the truth, but that it is “all about probabilities” [S10]. However, he also commented on the diminishing returns of additional information or situations of too much information [S10]. One participant commented on the necessary compromise between clarity and the amount of information displayed [S1].

A large group of participants stated that they use the probability of a prediction and its visualization as an indicator to make their decision [E2, E3, E5, S1, S10]. The display of probabilities was seen as a big improvement [S1]. People noted that seeing the probability makes it possible to decide whether something has a high probability or whether a prediction is just due to chance [S8]. Not knowing about the probability distribution was considered to be a problem with some of the visualizations [S8, S9]. Besides looking at the probabilities, counting errors or counting correct classifications were commonly cited ways to assess the accuracy of an ML system [E1, S1, S5, S7, S9]. Participants also used the frequency of the errors [E1] and their severity [S3]. Some participants explicitly framed this as comparing the system accuracy to their accuracy at the task [E4, S5, S7]. For one, errors confirmed that the system has trouble with the prediction task [S10]. Some participants found it hard to determine the accuracy of the system and commented on the difficulty and complexity of the task [E1, S4, S10]. One participant remarked that the visualizations only provided a snapshot of the accuracy of the system, which led him to still have doubts about the overall accuracy of the system [S3]. Another participant commented that the speed of the assessment of the system performance is most important to him [E5]. A large group also viewed it positively when the wrong predictions were at least plausible for them as humans [E5, S1, S3, S6, S9]. Animals, for example, should yield other animals [E5, S1, S6]. Mistaking a cat for a dog was considered a less severe error [S6] and better than mistaking a cat for an airplane [S1]. A complete mismatch between the predicted classes and the true classes led to the system being perceived as being incorrect and faulty [S9]. For situations where more than one prediction was shown, the cognitive load was considered higher since the user had to reason about the semantic similarity of the different categories [S9]. If a visualization provided a ranking, participants used their decisions based on whether the top prediction was correct [S8]. For a visualization that also showed the probability of the decision respectively the confidence of the system, the criterion was whether the probability was higher than 50 percent [S8].

The third research question was how the visualizations and the accuracy of the ML system affect trust and reliance. In the following, we will, therefore, explore how the participants differentiated between trust and reliance in the interviews. A large fraction of our participants equaled trust to accuracy [E2, E5, S1, S2, S4, S7, S10]. They saw trust to be based on observing a mismatch between the prediction of the system and their classification of the image [E1], a function of accuracy [E5], or somehow connected to accuracy [S5]. For one participant, the expectation that the results are correct equals trust [S4]. Other participants framed trust as high prediction accuracy [S7] or focused on a negative relationship where less accuracy equals less trust [E3, S1, S7]. The accuracy metric was seen as a way to build trust [S5]. Trust was described as giving up agency and letting the system make decisions on behalf of the user [S10]. One participant connected trust to feelings [S5]. This emotional perspective was also voiced by another participant, who connected trust to feelings and intuition [E4]. One participant described a moment where an error caused a breakdown that eroded his trust: “Suddenly, the moment that I found the first error in the system, I was like Oh! (...) it destroyed my trust. And after that, I could not trust it” [E3]. Other participants commented on how trust develops and improves through the understanding of a process [S2] and with time [S5, S6]. Participants also commented
on the connection between experience and trust [S6], that they have more trust in an existing system than in a new system [S5], and that knowing a system influences both trust and reliance [S5]. When asked to distinguish between relying on the predictions of a system and trusting a system, many participants regarded trust and reliance in a system as the same [E2, S4, S7, S8], mostly the same [S10], or similar [S1, S2]. Three participants made a difference between trust and reliance [E5, S3, S5]. They stated that in some cases, trust is not the same as reliance [S5], even though the difference is not clear [E5]. Regarding the relationship between trust and reliance, one participant said that when “I rely on it, I trust it” [S4]. Another participant said that he would rely on a system, but he would not trust it [S6]. Others said that trust comes first and reliance second [E3, S8]. One of the participants regarded trust as a necessary condition for reliance [S8]. Reliance was also described as not checking again whether something is correct [S5]. One participant made the distinction of reliance as technical and trust as emotional [S6].

5 DISCUSSION

The results show that participants prefer visualizations that expose the statistical nature of ML systems by indicating the probability distribution of the Top-3 predictions over action-oriented visualizations that only show the top prediction. This has important implications for interactive machine learning and applications where users are directly and indirectly training machine learning systems. Such systems should expose the probabilities computed by the machine learning systems. With this, we extend on recent research that studies algorithmic experience and awareness [2, 9, 15]. Our results also connect to Eslami et al.’s finding that users can detect algorithmic bias during their regular usage of a service [10].

A trustworthy visualization for an object recognition system should support the strategies that participants apply to distinguish between the systems. The most important strategies to determine the accuracy were interpreting the probabilities and counting the errors. For both, participants took the severity of errors into account. Regarding the helpfulness of visualizations, participants frequently commented on the appropriate amount of information. In the interviews, trust and reliance were strongly linked to accuracy. Further research should explore whether directly rating the accuracy of an ML system is the most straightforward way to measure the quality of an ML system or whether experiential qualities like trust and reliance capture more than mere accuracy. Our interviews showed that participants not only focus on accuracy but that they also take the perceived plausibility and severity of misclassification into account. It would, therefore, be interesting to see how ratings of trust extend on ratings of accuracy by accounting for the unexpected mistakes that ML systems can make. Our findings show that it may not be sufficient to merely improve the accuracy of an ML system. In the interviews, participants argued that mistaking a cat for a dog was better than mistaking a cat for an airplane [S6] and that animals should yield other animals [E5]. This implies that a semantically plausible error is regarded as more tolerable than a semantically unrelated error. Whether machine learning systems that fail in ways that humans consider semantically plausible are preferable remains an important open question. Our results indicate that the kinds of errors an ML system makes could be an important way to increase trust in an ML system. Optimizing the plausibility of errors and designing the error cases could be an alternative to explanations of the decisions of machine learning systems. This connects to Gregor et al., who argue that explanations are needed when unexpected behavior like anomalies occur [13]. Anomalies, by definition, are hard to anticipate or to understand. Trust is aimed at situations where a complete understanding is impractical [6, 23]. Rather than aiming to explain how decisions are made [32, 36, 37], the plausibility of the ML predictions could be a straightforward way to communicate to users that they can trust and rely on a system in use. The types of errors a machine learning system makes could be designed to signal system accuracy. Plausible errors could increase trust in an ML system, while implausible errors could lead to distrust. The objective function of a neural network could be adapted to penalize errors that users regard as plausible and reward errors that users perceive as implausible. This could convey the system accuracy through the predictions of the machine learning system [11]. We also found that visualizations that show the probability of the predictions are preferred over rankings of the results. The interviews revealed the strategies that participants use to assess the performance of ML systems and what participants think they need in a visualization. When assessing ML systems that classify images, participants take the severity of an error and its likelihood into account. Semantically plausible errors are more tolerable than those that are seemingly random. We also found that the participants in our investigation did not want simple answers or recommendations they can follow. In conclusion, this means that trustworthy machine learning interfaces should show an appropriate amount of information, account for unexpected errors, and expose how the system works. Errors of the system could be used to communicate system performance. Semantically implausible errors, like a cat that is misclassified as an airplane, could be used to alert users about situations where a system is not trustworthy.

REFERENCES

[1] Kamal Ahmed. 2015. Google apologises for racist blunder. BBC News (July 2015). https://www.bbc.co.uk/news/technology-33347866
[2] Oscar Alvarado and Annika Waern. 2018. Towards Algorithmic Experience: Initial Efforts for Social Media Contexts. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI ’18). ACM, New York, NY, USA, Article 286, 12 pages. https://doi.org/10.1145/3173574.3173860
[3] Saleema Amershi, Maya Cakmak, William Bradley Knox, and Todd Kulesza. 2014. Power to the people: The role of humans in interactive machine learning. AI Magazine 35, 4 (2014), 105–120.
[4] Mariusz Bojański, Davide Del Testa, Daniel Dworakowski, Bernhard Firner, Beat Flepp, Prasoon Goyal, Lawrence D Jackel, Mathew Monfort, Urs Muller, Jiakai Zhang, et al. 2016. End to end learning for self-driving cars. arXiv preprint arXiv:1604.07316 (2016).
[5] Eun Kyoung Choe, Nicole B. Lee, Bongshin Lee, Wanda Pratt, and Julie A. Kientz. 2014. Understanding Quantified-sellers’ Practices in Collecting and Exploring Personal Data. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’14). ACM, New York, NY, USA, 1143–1152. https://doi.org/10.1145/2556288.2557372
[6] Henriette S.M. Cramer, Vanessa Evers, Maarten W. van Someren, and Bob J. Wielinga. 2009. Awareness, Training and Trust in Interaction with Adaptive Spam Filters. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI ’09). ACM, New York, NY, USA, 909–912. https://doi.org/10.1145/1518701.1518839
[7] J. P. Djajadiningrat, W. W. Gaver, and J. W. Fes. 2000. Interaction Relabeling and Extreme Characters: Methods for Exploring Aesthetic Interactions. In Proceedings of the 3rd Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques (DIS ’00). ACM, New York, NY, USA, 66–71. https://doi.org/10.1145/347642.347664
