GANterfactual-RL: Understanding Reinforcement Learning Agents’ Strategies through Visual Counterfactual Explanations

Tobias Huber
University of Augsburg
Augsburg, Germany
tobias.huber@uni-a.de

Maximilian Demmler
University of Augsburg
Augsburg, Germany
maxdemmler@googlemail.com

Silvan Mertes
University of Augsburg
Augsburg, Germany
silvan.mertes@uni-a.de

Matthew L. Olson
Oregon State University
Corvallis, OR, United States
olsomatt@oregonstate.edu

Elisabeth André
University of Augsburg
Augsburg, Germany
andre@informatik.uni-augsburg.de

ABSTRACT
Counterfactual explanations are a common tool to explain artificial intelligence models. For Reinforcement Learning (RL) agents, they answer “Why not?” or “What if?” questions by illustrating what minimal change to a state is needed such that an agent chooses a different action. Generating counterfactual explanations for RL agents with visual input is especially challenging because of their large state spaces and deep learning algorithms, making the decisions of RL agents more challenging. For one, RL agents are not isolated. These actions are part of a long-term strategy that might be influenced by delayed rewards. Secondly, RL agents are not able to understand the agents to enable appropriate use of them and to facilitate human-agent cooperation [37]. One prominent paradigm to make the decisions of intelligent agents transparent and comprehensible is the Counterfactual Explanations paradigm. By providing an alternative reality where the agent would have made a different decision, these explanations follow a rather human way of describing decisions [4, 27]. For example, if a person would have to explain why a warehouse robot took a detour instead of directly moving to its desired target, they would probably give an explanation similar to “If there was no production worker in the way, the robot would have moved straight to its target - and, by doing so, give a counterfactual explanation of the warehouse robot’s behavior. Figure 1 shows a similar situation from the Atari game Pacman.

Figure 1: Example for a counterfactual explanation: In the original situation (a), the agent does not take the fastest path to the pill in the top right corner. It is unclear if the agent is afraid of the ghost or does not recognize the shortest path. The counterfactual state (b) shows that the agent would have taken the fastest path to the pill if the ghost was not there. This indicates that the agent is afraid of the ghost.

1 INTRODUCTION
Modern Reinforcement Learning (RL) agents use increasingly complex state spaces and deep learning algorithms, making the decisions and strategies of such agents hard to understand [15]. At the same time, these deep RL agents are being deployed into increasingly high-risk domains like healthcare, autonomous driving, and robotic navigation [11, 21, 43]. In such domains, it is crucial to be able to understand the agents to enable appropriate use of them and to facilitate human-agent cooperation [37]. One prominent paradigm to make the decisions of intelligent agents transparent and comprehensible is the Counterfactual Explanations paradigm. By providing an alternative reality where the agent would have made a different decision, these explanations follow a rather human way of describing decisions [4, 27]. For example, if a person would have to explain why a warehouse robot took a detour instead of directly moving to its desired target, they would probably give an explanation similar to “If there was no production worker in the way, the robot would have moved straight to its target - and, by doing so, give a counterfactual explanation of the warehouse robot’s behavior. Figure 1 shows a similar situation from the Atari game Pacman.

In other machine learning domains, such as image classification, counterfactual explanations are already frequently used. However, this is not the case for RL, as several factors make explaining the decisions of RL agents more challenging. For one, RL agents are used for sequential decision-making tasks: their actions are part of a long-term strategy that might be influenced by delayed rewards. Secondly, RL agents are not trained on a given ground truth strategy. The reward function only indirectly specifies the agent’s goals [10]. The emerging strategies
might not be what humans would expect, even if the strategy is optimal for the reward function. Finally, for RL agents, there is no direct counterpart to the training datasets used by supervised models. Therefore, counterfactual explanation approaches for supervised models that utilize the training data cannot be applied to RL agents without adjustment [41].

Due to the difficulties mentioned above, there is only one approach that focuses on creating counterfactual explanations for deep RL agents with visual input [32]. This approach utilizes a complex combination of models where the final generator is only indirectly trained to change the action. Olson et al. [32] show that their approach can be applied to a variety of RL environments and helps users identify a flawed agent. With the help of their counterfactual explanations, users were able to differentiate between a normal RL agent for the Atari game Space Invaders and a flawed agent that did not see a specific in-game object. For this task, it is sufficient for the counterfactual explanation to not change the particular object at all while other objects frequently change. This clearly communicates that the unchanged object is irrelevant and ignored by the agent, implying that it is not seen at all.

But for counterfactual explanations to be employed more widely, they also have to be useful for more complex tasks. According to Hoffman et al. [14], one of the main goals of a good explanation is to refine the user’s mental model of the agent. For RL agents, this includes understanding what strategy and intentions an agent pursues. Another critical goal for explanations is that they should help users to calibrate their trust in different agents [14]. For RL agents, this entails that users should be able to choose fitting agents for specific problems, which is more complex than simply identifying defective agents. The two aforementioned challenges require counterfactual explanations not only convey what objects need to change but also how the objects need to be altered to change the agents’ policy.

To tackle these challenges, this paper proposes a novel method for generating counterfactual explanations for RL agents with visual input. We do so by formulating the generation problem as a domain transfer problem where the domains are represented by sets of states that lead the agent to different actions. Our approach is fully model-agnostic, easier to train than the approach presented by Olson et al., and includes the counterfactual actions more directly into the training routine by solving an action-to-action domain transfer problem. We evaluate our approach with computational metrics (e.g., how often do the counterfactuals change the agent’s decision) and a user study using the Atari Learning Environment (ALE) [3], a common benchmark for RL agents with visual input. In our user study, we present participants with different kinds of counterfactual explanations and investigate whether this helps them to understand the strategies of Pacman agents. Furthermore, we investigate if the counterfactuals help them to calibrate their trust, so they can choose fitting agents for specific tasks (surviving or receiving points).

As such, the contributions of this paper are as follows: We formulate a novel, model-agnostic approach for generating counterfactual explanations for RL agents. We demonstrate that our approach outperforms the previous method in several computational metrics. Furthermore, we conduct a user study that shows, for the first time, that counterfactual explanations can help to understand the strategies of RL agents. This user study also identifies current deficiencies of counterfactual explanations for RL agents that point the way for future work.

2 RELATED WORK

Our work deals with post-hoc explanations that are generated for fully trained black-box agents. Recent years saw a plethora of work on such explanations for (deep) RL agents. The literature often divides them by scope into global and local explanations. Global explanations try to explain the agent’s overall strategy. This can be done by picking a subset of important state-action pairs that summarize the agent’s strategy [1, 15] or by distilling the agent’s policy into a simpler model like a finite state machine [8] or a soft decision tree [7]. In this paper, we focus on local explanations that explain a specific decision of an agent. The most common approach to local explanations for RL agents are Feature Attribution or Saliency Map methods [18, 34, 44]. These methods try to identify the most important input features for a specific decision and highlight them, for example in a heatmap. However, recent work questioned whether one can rely on post-hoc feature attribution to faithfully represent the agent’s internal reasoning [2, 17]. Furthermore, previous studies showed that saliency maps for visual RL agents are hard to understand for end-users [19]. Counterfactual explanations are another type of local explanation. Since they follow the human thinking paradigm of counterfactual reasoning, it is often argued that they are easier to interpret than feature attribution methods [4, 27].

For classification models, there is a growing body of work on counterfactual explanations. In 2017, Wachter et al. [39] were the first to introduce counterfactual explanations into the XAI domain by defining them as an optimization problem. Since then, various approaches to generate such counterfactuals were proposed, e.g., van Looveren and Klaise [23], and [12].

As various research has observed that generating counterfactual explanations is, at its core, a generative problem, the use of generative models like Generative Adversarial Networks (GANs) quickly became prevailing in state-of-the-art counterfactual explanation generation algorithms. E.g., Németh et al. [31] proposed CounterGAN, a framework to build highly realistic and actionable counterfactual explanations. Zhao et al. [45] propose an approach for generating counterfactual image explanations by using text descriptions of relevant features of an image to be explained. Furthermore, various specialized GAN-based algorithms were introduced to generate counterfactual explanations in the medical domain [24, 25, 38]. More recent frameworks for counterfactual explanation generation make use of the StyleGAN architecture, which implicitly models style-related aspects of an image, which makes it perfectly suitable for a whole range of image classification tasks [22, 35]. As for a broad range of use cases, it is essential to be able to provide explanations for multiple counter-classes, various approaches have focused on that particular capability by using architectures based on StarGAN, an adversarial framework that was specifically designed for image translation between multiple domains [42, 46]. One drawback of the aforementioned approaches for supervised learning is that their GANs are trained to transfer between domains given by the labeled classes from the classifier’s training dataset.
Then they add additional measures (e.g., loss functions [25, 46]), to ensure that the generated counterfactuals are actually classified as the desired class by the classifier that is to be explained. This is not possible for RL agents that do not have a training set. Furthermore, the additional measures are often not model-agnostic.

RL is often used to create counterfactual explanations for other models (for example in [5]). However, to the best of the authors’ knowledge, there is only one previous work on generating visual counterfactual explanations for RL agents [32]. Olson et al. [32] train an encoder $E$ that creates an action-invariant latent representation of the agent’s latent space. This is achieved by adversarially training $E$ in tandem with a discriminator $D$, where $D$ tries to predict the agent’s action and $E$ aims to make the decision of $D$ as uncertain as possible. In addition, they train a generative model $G$ to replicate states $s$ based on the action-invariant latent representation $E(s)$ and the agent’s action probability distribution $\pi(s)$ for this state. By providing $G$ with a counterfactual action distribution $\pi(s')$, they obtain a state that is similar to $s$ but brings the agent’s action distribution closer to the desired counterfactual distribution. However, Olson et al. argue that an arbitrary counterfactual action distribution does not represent a realistic agent output and thus leads to unrealistic counterfactual states. To avoid this, they train an additional Wasserstein Auto Encoder and use it to perform gradient descent in the latent space of the agent towards an agent output that resembles the desired counterfactual action. Olson et al. refer to their approach as Counterfactual State Explanations (CSE), therefore we will also refer to it as CSE in this paper.

The CSE approach is fairly complex and requires extensive access to the agent’s inner workings. Furthermore, as Olson et al. mention themselves, the loss function of the generator $G$ does not directly force the resulting state $G(E(s), \pi(s'))$ to be classified as the counterfactual action distribution $\pi(s')$. This is only learned indirectly by replicating states based on the action-invariant latent space and the desired action distribution $\pi(s')$. As we show in Section 4, this does not seem to be enough to change the agent’s decision correctly. To solve those problems, we formulate a simpler counterfactual generation method that uses the counterfactual actions in a more direct way.

3 APPROACH

3.1 GANterfactual-RL

RL agents are usually employed in a Markov Decision Process (MDP) which consists of states $s \in S$, actions $a \in A$, and rewards $r$. Given a state $s$, the goal of an RL agent $\pi : S \rightarrow A$ is to choose an action $\pi(s)$ that maximizes its cumulative future rewards. To explain such an agent, the objective of a counterfactual explanation approach for RL agents is defined as follows. Given an original state $s$ and a desired counterfactual action $a'$, we want a counterfactual state $s'$ that makes the agent choose the desired action $\pi(s') = a'$. Hereby, the original state $s$ should be altered as little as possible. On an abstract level, the action $\pi(s)$ that the agent chooses for a state $s$ can be seen as a top-level feature that describes a combination of several underlying features which the agent considers to be relevant for its decision. Thus, the counterfactual state $s'$ should only change the features that are relevant to the agent’s decision, while maintaining all other features not relevant to the decision.

This is similar to image-to-image translation, where features that are relevant for a certain image domain should be transformed into features leading to another image domain, while all other features have to be maintained (e.g., the background should remain constant when transforming horses to zebras). Taken together, we can formulate the generation of counterfactual states for RL agents as a domain transfer problem similar to image-to-image translation: The agent’s action space $A$ defines the different domains $A_j = \{s \in S | \pi(s) = a_j\}$, where each state belongs to the domain that corresponds to the action that the agent chooses for this state (see Figure 2).

To solve the reformulated domain transfer problem, we base our system on the StarGAN architecture [6], since RL agents usually use more than two actions. The StarGAN architecture incorporates multiple loss components that can be reformulated to be applicable to the RL domain. The first component, the so-called adversarial loss, leads the network to produce highly realistic states that look like states from the original environment. Reformulated for the task of generating RL states, we define it as follows (following Choi et al. [6] we use a Wasserstein objective with gradient penalty):

$$L_{adv} = \mathbb{E}_s [D_{src}(s)] - \mathbb{E}_{s,a'} [D_{src}(G(s,a'))] - \lambda_g \mathbb{E}_s \left[ || \nabla_s D_{src}(s) ||^2 - 1 \right]^2,$$

where $D_{src}$ is the StarGAN’s discriminator network and $G$ its generator network. The second loss component, which is specific to the StarGAN architecture, guides the generator network to produce states that lead to the desired counterfactual actions. It consists of two sub-objectives, one that is applied while the network is fed with original (real) states from the training set (Eq. 1), and the other while the network is generating counterfactual states (Eq. 2):

$$L_{cls}^u = \mathbb{E}_{s,a} [- \log D_{cls}(a|s)], \quad \text{(1)}$$

$$L_{cls}' = \mathbb{E}_{s,a,a'} [- \log D_{cls}(a'|G(s,a'))], \quad \text{(2)}$$

where $D_{cls}$ refers to the StarGAN discriminator’s classification output, which learns to approximate the action that the agent is performing in a particular state. Further, as counterfactual states should be as close to the original states as possible, a Reconstruction
Loss is used. This loss forces the network to only change features that are relevant to the agent’s choice of action:
\[
L_{rec} = \mathbb{E}_{s,a} [||s - G(s, a)||_1]
\]
Taken together, the whole loss of the StarGAN architecture, reformulated for RL counterfactual explanations, is defined as follows:
\[
L_D = -L_{adv} + \lambda_{cls} \mathbb{E}_{s,a} L_{cls}^a + \lambda_{rec} L_{rec}
\]
where \(\lambda_{cls}\) and \(\lambda_{rec}\) are weights controlling the corresponding loss component’s relevance. Since our approach utilizes a GAN architecture to generate counterfactuals for RL agents, we refer to it as GANterfactual-RL.

3.2 Dataset Generation
As described above, our GANterfactual-RL approach relies on training data in the form of state-action pairs. Olson et al. [32] train their CSE approach on state-action pairs generated by concurrently running an MDP with a trained agent. This strategy is simple but allows for little control over the training data, which can lead to the following complications:
- Frames extracted from a running MDP contain a temporal pattern since consecutive states typically have a high correlation. Such correlations and patterns can lead to bias and sub-optimal convergence during training.
- For episodic MDPs, there is a high probability of reaching the same state throughout several episodes. This is amplified by the fact that RL agents often learn to execute only a few optimal trajectories. This results in duplicate samples that are effectively over-sampled during training.
- RL agents generally do not execute each action equally frequently, since most environments contain actions that are useful more often than others. This leads to an imbalanced amount of training samples per domain.

To mitigate the aforementioned issues, we propose to generate datasets as follows: Data is gathered by running a trained agent in an MDP. Each state corresponds to one dataset sample and is labeled with the action that the agent chooses to execute in this state. An \(\epsilon\)-greedy policy (\(\epsilon = 0.2\) in our case) is used to increase the diversity of states reached over multiple episodes. State-action pairs with an explored (randomly chosen) action are not added to the dataset. After the data is gathered, duplicates are removed. Then, a class balancing technique (under-sampling in our case) is used to account for over- or underrepresented actions. Finally, the dataset is split into a training set, a test set, and potentially a validation set.

Most of these techniques are commonly used in other application domains of machine learning. However, to our best knowledge, this is the first work to generate and preprocess datasets for generating counterfactual explanations for RL agents.

3.3 Application to Atari Domain
Environment. The environments we use for our experiments are the Atari 2600 games MsPacman (henceforth referred to as Pacman) and Space Invaders, included in the Arcade Learning Environment (ALE) [3]. The ALE states are based on the raw pixel values of the game. Each input frame is cropped so that only the actual playing field remains. This removes components such as the score and life indicators which would allow participants to easily see which agent receives higher scores. After that, we use the same preprocessing as Mnih et al. [29]. Two steps from this preprocessing are particularly important for us. First, the frames are gray-scaled and downsized. Second, in addition to the current frame, the agent receives the last three preprocessed frames as input. This allows the agent to detect temporal relations. The ALE actions normally correspond to the meaningful actions achieved with an Atari 2600 controller (e.g. six actions for Space Invaders). Since we wanted to use our Pacman agents in a user study we removed 4 redundant actions (e.g., Up & Right) whose effect differs between situations and is therefore hard to convey to participants. This left us with 5 actions for Pacman (Do nothing, Up, Down, Left, Right).

Agent Training. To evaluate participants’ ability to differentiate between alternative agents and analyze their strategies, we modified the reward function of three Pacman agents. This is a more natural method of obtaining different agents compared to withholding information from the agent as Olson et al. [32] did. Furthermore, it results in agents that behave qualitatively differently. Therefore participants have to actually analyze the agents’ strategies instead of simply looking for objects that the agents ignore.
- **Blue-Ghost Agent**: This agent was trained using the default reward function of the ALE, where blue ghosts get the highest reward.
- **Power Pill Agent**: This agent only received positive rewards for eating power pills.
- **Fear-Ghost Agent**: This agent got a small positive reward of 1 for every step in which it did not die to ghosts.

For training the first two Pacman agents, we use the DQN algorithm [29]. Each agent was trained for 5 Million steps. The fear-ghost agent was trained using the ACER algorithm [40] for 10M steps. At the end of the training period, the best-performing policy is restored. For all three agents, we build upon the OpenAI baselines [9] repository. For Space Invaders, we used the two Asynchronous Advantage Actor-Critic (A3C) agents trained by Olson et al. [32]. For training details, we refer to their paper. One agent is trained normally, while the other agent is flawed and does not see the laser cannon at the bottom of the screen.

GANterfactual-RL on Atari. To generate human-understandable counterfactual explanations for our Atari agents, the generated counterfactual states should represent the frames that humans see during gameplay. That means we cannot train our GANterfactual-RL model on the preprocessed and stacked frames that the Atari agents use. Instead, we train it on the cropped RGB frames before preprocessing. The only preprocessing we still use on those frames is a countermeasure against flickering objects in Atari games, which was proposed by Mnih et al. [29]. While generating the dataset, we only save the most recent of the four stacked frames for each state \(s\). This frame generally influences the agent’s decision the most. For feeding the counterfactual frame back into the agent (e.g., to evaluate the approach), we stack it four times and then apply preprocessing.

Implementation details are described in the appendix (to be found in the authors’ version [16]). The full code is available online.¹

¹https://github.com/hcmlab/GANterfactual-RL
4 COMPUTATIONAL EVALUATION

4.1 Used Metrics

We evaluate our approach using the metrics validity (or success rate), proximity (or cost), sparsity, and generation time. We consider these metrics to be the most suitable and widely used metrics for image-based counterfactual explanations [5, 20, 30, 33].

Validity captures the rate of CounterFacts (CFs) that actually evoke the targeted action when fed to the agent. With $N_T$ being true CFs (correctly changing the agent’s action), $N_F$ being false CFs, and $N$ the total amount of evaluated CFs, this metric is defined as:

$$ Validity = \frac{N_T}{N_T + N_F} = \frac{N_T}{N} $$

Proximity measures the similarity between an original state image and its CF via the L1-norm. We normalize the metric to measure the proximity in the range $[0, 1]$.

$$ Proximity(s, G) = 1 - \frac{1}{255 \cdot S} \| s - G(s, a) \|_1 $$

where $s$ is the original state image, $G(s, a)$ is the generated CF for an arbitrary target action domain $a$ and $S$ is the domain of color values of $s$ ($S = 3 \cdot Width \cdot Height$ for RGB-encoded images). The normalization with $255 \cdot S$ assumes an 8-bit color encoding with color values in range $[0, 255]$. High proximity values are desirable since they indicate small adjustments to the original state.

Sparsity quantifies the number of unmodified pixel values between an original state image and its CF via the L0-norm (a pseudo-norm that counts the number of non-zero entries of a vector/matrix). The sparsity is normalized to the range $[0, 1]$ as well.

$$ Sparsity(s, G) = 1 - \frac{1}{S} \| s - G(s, a) \|_0 $$

A completely altered image has a sparsity of 0, an unmodified image has a sparsity of 1. High sparsity values are thus desirable.

Generation Time determines the time it takes to generate one CF with a trained generator, not including pre- or post-processing.

4.2 Computational Results

The computational results for the three Pacman agents are shown in Table 1 and the results for the two Space Invaders agents in Table 2. For the Pacman agents, we generated fully cleaned datasets (Section 3.2) and sampled 10% of each action for the evaluation test set. To show the contribution of our proposed dataset generation, we additionally trained a GANterfactual-RL model for the blue-ghost agent without the steps proposed in Section 3.2 and evaluated it on the test set from the clean dataset. This dropped the validity to 0.45 and sparsity to 0.50 ± 0.01 while the other values stayed comparable. To be more comparable to the results by Olson et al. [32], we do not remove duplicates from the Space Invaders datasets and do not apply class balancing. Here we create the test set by sampling 500 states for each action and removing all duplicates of these states from the training set. Our GANterfactual-RL approach outperforms the CSE counterfactuals in every single metric.

Figure 3 shows example counterfactual states. Our approach does not change the Laser Cannon (marked in blue) for the flawed agent, who does not see it, but changes it for the normal agent.

5 USER STUDY

5.1 Study Design

5.1.1 Research Question and Hypothesis. The research question for our study was which counterfactual explanations help users to understand the strategies of RL agents and help them to choose fitting
agents for a specific task. We hypothesized that our GANterfactual-RL method is more useful than the CSE method and is more useful than a presentation of the original states without counterfactuals. Further, we thought that the counterfactuals generated by the CSE approach might mislead participants due to the low validity of the generated counterfactual explanations (see Section 4). Therefore, we hypothesized that only providing the original states is more useful than adding CSE counterfactuals.

5.1.2 Dependent Variables and Main Tasks.

Agent Understanding Task. To measure whether participants understand the strategies of different agents and build a correct mental model of them, we used an agent understanding task inspired by Hoffman et al. [14] and Huber et al. [19]. Here, participants were presented with five states and the actions that the agent chooses in these states. This was done for each of the three Pacman agents described in Section 3.3 (one agent at a time). The states were selected by the HIGHLIGHTS-Div algorithm [1]. To this end, we let each trained agent play for additional 50 episodes and chose the most important states according to HIGHLIGHTS-Div. The resulting states show gameplay that is typical for the agent, without the need to manually select states that might be biased toward our approach. Based on these states (and additional explanations depending on the condition), participants had to select up to two in-game objects that were most important for the agent’s strategy from a list of objects (Pacman, normal pills, power pills, ghosts, blue ghosts, or cherries). As described in Section 3.3, each agent, strongly focuses on a different single in-game object depending on their reward function (e.g., the fear-ghosts agent focuses on normal ghosts). If the participants select this object and none of the other objects, they receive a point. The only exception is Pacman. Every agent heavily relies on the position of Pacman as a source of information. Therefore, participants receive the point whether they select Pacman or not.

Agent Comparison Task. To measure how well the participants’ trust is calibrated, we used an agent comparison task inspired by Amir and Amir [1] and Miller [28]. Here, we implicitly measure if the participants’ trust is appropriate by asking them, for each possible pair of the three Pacman agents, which agent they would play on their behalf to obtain certain goals. Since a single agent can be good for one goal but bad for another, this requires a deeper analysis than the distinction between a normal and a defective agent. For each pair, the participants are shown their own descriptions of each agent from the agent understanding task and the same states and explanations that they saw during the agent understanding task. Then they have to decide which agent should play on their behalf to achieve more points and which agent should play on their behalf to survive longer. We know the ground truth for this by measuring the agents’ average score and amount of steps for the 50 episodes used to find the HIGHLIGHTS states. The amount of steps that the blue-ghost agent and the power pill agent survive is so close that we do not include this specific comparison in the evaluation.

Explanation Satisfaction. To measure the participant’s subjective satisfaction, we use statements adapted from the Explanation Satisfaction Scale by Hoffman et al. [14]. Participants have to rate their agreement with each statement on a 5-point Likert scale. Participants’ final rating was averaged over all those ratings, reversing the rating of negative statements. We do this once after the agent understanding task and once after the agent comparison task in case there are satisfaction differences between the tasks.

5.1.3 Conditions and Explanation Presentation. We used three independent conditions, one Control condition without explanations and two conditions where the states during the agent understanding task and the agent comparison task are accompanied by counterfactual explanations. In the CSE condition, the counterfactuals are generated by the approach from Olson et al. [32], and in the GANterfactual-RL condition the counterfactuals are generated by our proposed method. The presentation of the counterfactual explanations is designed as follows. For each state, we generate a single counterfactual state. We were concerned that too many counterfactual states would cause too much cognitive load. The way that MsPacman is implemented, actions that do nothing or move directly into a wall are ignored. To generate meaningful counterfactual states, we limited the counterfactual action to turning around in a corridor and randomly selecting a new direction at an intersection (do not turn around). The counterfactual states are presented by a slider under each state. Moving the slider from left to right linearly interpolates the original state to the counterfactual state (per-pixel interpolation). The original and counterfactual actions are written above the state. Figure 4 shows a simplified version of the beginning of our agent understanding task.

5.1.4 Procedure and Compensation. After completing a consent form, participants were asked to answer demographic questions (age and gender) and questions regarding their experience with Pacman and their views on AI. Then, they were shown a tutorial explaining the rules of the game Pacman and were asked to play the game to familiarize themselves with it. To verify that participants understood the rules, they were asked to complete a quiz and were only allowed to proceed with the survey after answering all questions correctly. Afterward, participants in the counterfactual conditions received additional information and another quiz regarding the counterfactual explanations. Then, they proceeded to the agent understanding task which was repeated three times, once for each agent. The order of the agents was randomized. After that,
participants filled the explanation satisfaction scale and continued
to the agent comparison task. Again, this task was repeated three
times, once for each possible agent pair, and the order was random-
ized. Finally, participants had to complete another satisfaction scale
for the agent comparison task. Participants got a compensation of
S$5 for participating in the study. As an incentive to do the tasks
properly, they received a bonus payment of 10 cents for each point
they get in the agent understanding task and 5 cents for each point
in the agent comparison task. The complete questionnaire can be
seen in the appendix [16]. We preregistered our study online.²

5.1.5 Participants. We recruited participants through Amazon Me-
chanical Turk. Participation was limited to Mechanical Turk Mas-
ters from the US, UK, or Canada (to ensure a sufficient English level)
with a task approval rate greater than 95% and without color vision
impairment. We conducted a power analysis with an estimated
medium effect size of 0.7 based on previous similar experiments
[19, 25, 26]. This determined that we need 28 participants per con-
dition to achieve a power of 0.8 and a significance level of 0.05. To
account for participant exclusions, we recruited 30 participants per
condition. Participants were excluded if they did not look at any of
the counterfactual explanations for any of the agents during the
agent understanding task, if their textual answers were nonsensical
or if they took considerably less time than the average. This left us
with 30 participants in the Control condition, 28 participants in the
CSE condition, and 23 in the GANterfactual-RL condition.

The distribution of age, AI experience, and Pacman experience
was similar between the conditions (see the appendix Huber et al.
[16]). There was a difference in the gender distribution and the
attitude towards AI between the conditions. The Control condition
had 40% female participants, the CSE condition had 32% and the
GANterfactual-RL condition had 26%. The mean attitude towards AI
was the highest in the GANterfactual-RL condition and the lowest
in the Control condition (see the appendix [16]).

5.2 Results
The results for the participants’ scores during the main tasks can
be seen in Figure 5, while their explanation satisfaction values are
shown in Figure 6. In the following, we will summarize the results
of our main hypotheses, which we analyzed using non-parametric
one-tailed Mann-Whitney U tests.

Counterfactuals helped participants to understand the
agents’ strategies. In the agent understanding task, there was
a significant difference between the Control condition (M=0.8)
and the GANterfactual-RL condition (M=1.65), U=181, p=0.001,
r=0.477.³ Contrary to our hypothesis, the Control condition got
lower scores than the CSE condition (M=0.8 vs M=1.18), p=0.953.

Our GANterfactual-RL explanations were significantly
more useful than the CSE approach for understanding the
agents’ strategies. In the agent understanding task, the CSE condi-
tion got a mean score of 1.18, while the GANterfactual-RL condition
got a mean score of 1.65 (U=232, p=0.038, r=0.2795).

The increased understanding of the agents’ strategies did
not result in a more calibrated trust. Contrary to our hypothesis,
there were no significant differences in the trust task (Control

³https://aspredicted.org/m9ffs.pdf
³M is the mean and r is rank biserial correlation.

vs CSE: p=0.536, Control vs. GANterfactual-RL: p=0.852, CSE vs
GANterfactual-RL: p=0.876).

Counterfactuals did not increase explanation satisfaction.
Even though participants objectively had a better understanding of
the agents’ strategies, they did not feel more satisfied with them.
Participants in the Control condition were significantly more satis-
fied than participants in the CSE condition in both the agent un-
derstanding task (Control: M=3.77, CSE: M=3.20; U=249, p=0.004,
r=0.4071) and the agent comparison task (Control: M=3.75, CSE:
M=3.14; U=267, p=0.008, r=0.3643). Contrary to our expectations,
the participants in the GANterfactual-RL condition were not more
satisfied than the participants in the Control condition or the
CSE condition in both the agent understanding task (Control vs.
GANterfactual-RL: p=0.996, CSE vs GANterfactual-RL: p=0.546) or
the agent comparison task (Control vs. GANterfactual-RL: p=0.967,
CSE vs GANterfactual-RL: p=0.334).

6 DISCUSSION
6.1 Computational Evaluation
Our computational evaluation shows that our proposed approach is
correctly changing the agents’ actions in 46% to 70% of the cases de-
pending on the agent. While this is not perfect, one has to consider
that this is not a binary task but that the agents have 5 or 6 different
actions. Furthermore, CSE [32], the only previous method that fo-
cuses on generating counterfactual explanations for RL agents, only
successfully changed the agent’s decision in 17% to 28% of the cases.
We can think of two reasons for the low validity values for the CSE
approach. First, they only incorporate the agent’s action in their
loss functions related to the latent space (where their discriminator and WAE were trained). The generation of the final pixels did not include constraints to faithfully ensure that a specific action was taken by the agent. Second, their loss functions for the latent space focus on creating action-invariant states. Olson et al. [32] showed that their CSE approach was useful for differentiating between a normal agent and a flawed agent. We think this is due to the fact that CSE is good at generating action-invariant states. This can help to identify the object that the flawed agent did not see since irrelevant objects are not changed for action-invariant states. We found that our approach also does not change the irrelevant object for the flawed agent (illustrated in Figure 3). This demonstrates that the counterfactual states generated by our approach are similarly effective for identifying the flawed agent. Looking at the distance between the original and the counterfactual states in pixel-space, we see that counterfactual states generated by our GANterfactual-RL approach on average have less distance to the original states and change fewer pixel values compared to the counterfactuals generated by the previous CSE method by Olson et al. [32]. This indicates that our GANterfactual-RL method is better at achieving the goal of finding the smallest possible modification of the original state to change the agent’s decision. Since our method only requires a single forward pass to generate a counterfactual state, it is faster than the CSE method, which relies on potentially time-consuming gradient descent for the counterfactual generation.

### 6.2 User Study

Our user study showed that counterfactual explanations help users to understand which strategies different agents pursue. In particular, our method was significantly more useful than both the CSE method and not providing counterfactuals. Contrary to our hypothesis, even the counterfactuals generated by the CSE method resulted in a better understanding of the agents than not providing counterfactual explanations. This demonstrates the usefulness of counterfactual explanations for RL agents even in more complex tasks than identifying defective agents. Two recent studies evaluated the usefulness of other explanation techniques for understanding the strategies of RL agents in a similar way to our study. Huber et al. [19] looked at saliency map explanations and found that they did not help more than showing HIGHLIGHTS states without saliency maps. Their participants achieved 37% of the maximum possible score in their agent understanding task, while the participants with our counterfactual explanations obtained 50%. Septon et al. [36] investigated so-called reward decomposition explanations and found that they helped participants to achieve 60% of the maximum score in their agent understanding task. However, reward decomposition is an intrinsic explanation method which the agent and the reward function have to be specifically designed for. Our counterfactual explanations resulted in only 10% less average score even though they are post-hoc explanations that can be generated for already trained black-box agents.

Our agent comparison task showed that the increased understanding of the agent’s strategies through both counterfactual explanation methods did not help participants choose fitting agents for specific tasks. For choosing the correct agent for a given problem, it is not enough to identify the strategies of the agents. It also requires enough expertise in the environment (e.g., Pacman) to judge which strategy is better suited for the problem at hand. For example, in Pacman, humans often assume that an agent that survives longer will accumulate more points in the long run. However, this is not necessarily the case since an aggressive agent can better exploit the very high rewards of eating blue ghosts. Our results for this task are in line with the results of the agent comparison task for saliency maps by Huber et al. [19].

Finally, our study showed that participants subjectively were not satisfied with the counterfactual explanations even though they objectively helped them to understand the agents. This might be due to the additional cognitive load of interpreting the explanations. The two aforementioned studies [19, 36] also did not find a significant difference in user satisfaction for their local explanation techniques. Only the choice of states, which does not provide additional information, influenced the satisfaction in [19]. However, our study is the first to see significantly higher satisfaction for the no-explanation condition than one of the two explanation conditions. This indicates that counterfactuals are subjectively less satisfying than saliency maps or reward decomposition. One possible explanation for this is the visual quality of the counterfactuals. Some participants from both counterfactual conditions commented that the counterfactuals had too many artifacts. One participant from the GANterfactual-RL condition for example wrote that “The counterfactuals were somewhat helpful, but they would have worked better if there were fewer or no artifacts”. Another possible reason for the low satisfaction is the presentation of the explanation. Because our study primarily aimed at investigating the benefits and drawbacks of our specific counterfactual approach, we did not use a user-friendly explanatory system where different types of explanations are provided according to the requests of the explainee.

### 7 Conclusion and Future Work

In this work, we formulated a novel method for generating counterfactual explanations for RL agents. This GANterfactual-RL method is fully model-agnostic, which we demonstrate by applying it to three RL algorithms, two actor-critic methods, and one deep Q-learning method. Using computational metrics, we show that our proposed method is better at correctly changing the agent’s decision while modifying less of the original input and taking less time than the only previous method that focuses on generating visual counterfactuals for RL. Furthermore, it significantly improved users’ understanding of the strategies of different agents in a user study.

Our user study also identified two remaining deficiencies of counterfactual explanations. First, participants were subjectively not satisfied with the explanations, which might be due to unnatural artifacts in some counterfactuals. Second, the counterfactuals did not help them to calibrate their trust in the agents. Future work should try to improve counterfactual explanations in these directions.

While there is still room for improvement, we can confidently say that our approach can be considered the current state of the art for counterfactual explanations for RL agents with visual input.

**Acknowledgments**

This paper was partially funded by the DFG through the Leibniz award of Elisabeth André (AN 559/10-1).


