International Journal of Computer Science and Information Technology
ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 4, Number 3, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v4n3.19
Journal homepage: https://wepub.org/index.php/IJCSIT/index

The Impact of Artificial Intelligence's Automatic Targeting on Traditional Online Games Cheating

Yixuan Hu

University of Birmingham, Birmingham B15 2TT, United Kingdom

ABSTRACT

With the continuous enhancement of people's spiritual pursuits, multiplayer online games have become a popular trend, encompassing both multiplayer cooperative and competitive games. In multiplayer competitive games, skill disparities among players can lead to unfair competition, prompting some players to resort to cheating for an advantage. Traditional cheating methods, such as memory injection to modify game data, while effective, are easily detectable. In recent years, with the rapid development of Artificial Intelligence (AI) technology, AI-based image recognition cheating software has emerged as a new trend. This software analyzes game screens to identify enemy positions and simulates human operations for automatic aiming, making it difficult for anti-cheating systems to detect. However, AI cheating software has high hardware requirements and is affected by game environments, such as smoke grenades and walls, which can limit its effectiveness. This study aims to explore the advantages and limitations of AI image recognition cheating software compared to traditional memory injection cheating software, analyze the extent of players' use of AI cheating software, and discuss strategies for game companies to combat such cheating behaviors. The research finds that AI cheating software offers superior concealment compared to traditional methods but comes with higher costs and usage barriers. Game companies can employ various measures to prevent cheating, including uploading files to servers for detection, monitoring background software, and using AI to detect abnormal mouse movements. Furthermore, the power of the gaming community should not be overlooked, as player supervision and reporting can effectively reduce cheating behaviors.

KEYWORDS

AI cheating software; Image recognition; Multiplayer online games; Memory injection

1. INTRODUCTION

With people's continuous pursuit of spirit, video games have become a trend among people. In this case, multiplayer games will become a relatively mainstream gameplay. This includes two types of multiplayer cooperative games and competitive games. An example of a typical multiplayer competitive game is Counter-Strike 1.6. Different people's reactions and external environments will lead to certain differences in the level of the game between players. There are two ways may decrease the gap between players. The first way is to practice more. This is a way that is acceptable to more players. However, another way, the problem we discuss below, is to become a hacker, which is also a way. An easily tools or a software who make by “hackers” will be a common way in game cheating. (Kanervisto et al., 2023). This is a mainstream way of cheating in the game. However, the staff of game companies will grow over time, and there are more and more ways to deal with this traditional way of cheating. The rapid development of artificial intelligence in the 21st century has made hackers see another way to cheat.

“Human-like gameplay” can be defined as artificially generated gameplay that is indistinguishable from genuine human gameplay, either by other humans or by automated detection systems. (Kanervisto et al., 2023) This cheating method is based on artificial intelligence and is different from traditional methods. It does not modify game files through memory scanning or memory injection, which reduces the probability of cheaters being found by anti-cheating software to a very low.

In the next report, will further explore some problems caused by artificial intelligence cheating software.

To what extent are artificial intelligence image recognition systems better than traditional memory injection cheating software in online gaming?

To what extent can online gaming players cheat with the use of AI image recognition systems?

To what extent do game companies have reasonable corresponding means to deal with this situation?

2. THE IMPACT OF ARTIFICIAL INTELLIGENCE'S AUTOMATIC TARGETING ON TRADITIONAL ONLINE GAMES CHEATING

2.1. To What Extent Are Artificial Intelligence Image Recognition Systems Better Than Traditional Memory Injection Cheating Software in Online Gaming?

Hackers have long leveraged the capabilities of reading and modifying game memory to inject cheating software into games. This technique allows them to ascertain the positions of enemy players and, more invasively, alter a player's health points or ammunition count for an unfair advantage. Such methods have remained a staple in the hacking community for their effectiveness but are notably prone to detection due to their direct interference with game data. (Kanervisto et al. 2023) While these traditional forms of cheating employ methods that are easily identifiable because of their intrusive nature, external hacks offer a different approach. Although modifying the player's blood volume or bullet count is easy to be recognized by anti-cheating programs, cheating based on the player's coordinates and identifying the cheating player is more difficult to detect. With the automatic mobile mouse program, it can provide very powerful unequal advantages to cheating players. However, with the continuous development of anti-cheating software, memory-based cheating software is becoming easier to identify. This will allow hackers to develop a new method of cheating to serve cheating players.

However, the advancement of artificial intelligence and computer vision (CV) technologies presents a new frontier for cheating in online games. These sophisticated CV hacks do not tamper with game data; instead, they analyze the images displayed to the player and extract information using techniques such as pixel color analysis, shape detection, and object recognition. (Kanervisto et al. 2023) Kanervisto note that upon identifying the target, these programs can simulate mouse movements to automatically aim at the enemy, thus facilitating cheating in a more concealed manner. This method's stealth is significantly enhanced by processing the screen captures on a separate computer from the one running the game, rendering anti-cheat programs unable to detect the rogue software. Furthermore, the simulation of mouse movements can be refined with randomization to mimic human behavior more closely, making this form of cheating particularly difficult to identify and, consequently, more harmful compared to traditional methods.

In essence, while traditional hacking methods remain detectable due to their intrusive nature, the evolution of AI and CV technologies offers a new paradigm for cheating. These advanced techniques provide a highly concealed and reliable means of gaining an unfair advantage in online gaming, posing a greater threat to the integrity of competitive play.

Certainly, cheating in online gaming through computer vision (CV) technology presents its unique challenges and limitations. In FPS games, players’ coordinates are intended to be confidential. When

a player is behind opaque objects like walls, it is presumed that other players cannot see them. However, to simplify implementation and enhance performance, most modern games synchronize every player's coordinates with each other. The visibility of blocked objects is managed by client-side software. (Detecting Passive Cheats in Online Games via Performance-Skillfulness Inconsistency, 2017). For instance, in a first-person shooter (FPS) game scenario, when a smoke bomb is deployed, visibility is drastically reduced for human players. This environmental effect equally impacts computer vision systems, which rely on visual data to operate. Just like human players, CV-based cheating tools cannot penetrate the visual obstruction caused by smoke to detect character models or other elements hidden behind the smokescreen. This inherent limitation significantly reduces the effectiveness of CV-based cheating mechanisms in such contexts.

Another pertinent example involves obstacles like walls within the game environment. Walls, similar to smoke bombs, create a physical barrier that obstructs the line of sight. For human players, enemies hidden behind walls remain unseen, preserving the element of surprise and strategy inherent in the game's design. This scenario parallels the limitations faced by CV cheating tools, which cannot visualize or recognize character models through solid obstacles.

However, this is where memory-injected cheating software comes into play, demonstrating a distinct advantage over CV-based tools. Unlike CV systems that rely on visual data, memory-injected cheats operate by accessing the game's memory directly. This approach allows them to bypass visual obstructions like walls or smoke bombs, enabling cheaters to spot enemies hidden behind barriers or within smoke clouds. This capability of memory-injected cheating software showcases a significant advantage over CV-based cheating, offering users an unfair competitive edge by revealing hidden opponents, thus undermining the game's fairness and competitive integrity.

Table 1. Memory-injected cheating software Vs CV-based cheating software

	memory-injected cheating software	CV-based cheating software
efficiency	Better	worse
stealthiness	worse	better
Cost	worse	better

2.2. To What Extent Can Online Gaming Players Cheat with the Use of AI Image Recognition Systems?

FPS games are the most popular e-sports games. However, the highly competitive nature of e-sports has resulted in the emergence of cheating tools. (Detection of a Novel Object-Detection-Based Cheat Tool for First-Person Shooter Games Using Machine Learning, 2023)

According to statistics from Steam, the world's largest gaming sales platform, the primary graphics cards owned by gamers are the RTX 3060, with a 6% ownership rate, and the GTX 1650, at 4.11%. When running Counter-Strike 2, these graphics cards are nearly fully utilized, with usage rates approaching 100%. This high level of resource consumption makes it challenging for most computer vision (CV) cheating software, which relies on GPU resources, to operate effectively. As a result, it is typically only players with higher-performance graphics cards who can use this type of cheating software. In contrast, the performance demands of memory-injected cheating software are significantly lower than those of CV cheating software, since it only needs to circumvent the game company's anti-cheating measures to read memory and obtain useful information for hackers. Consequently, the cost of using CV cheating software is higher, which in turn reduces its usage among the gaming community.

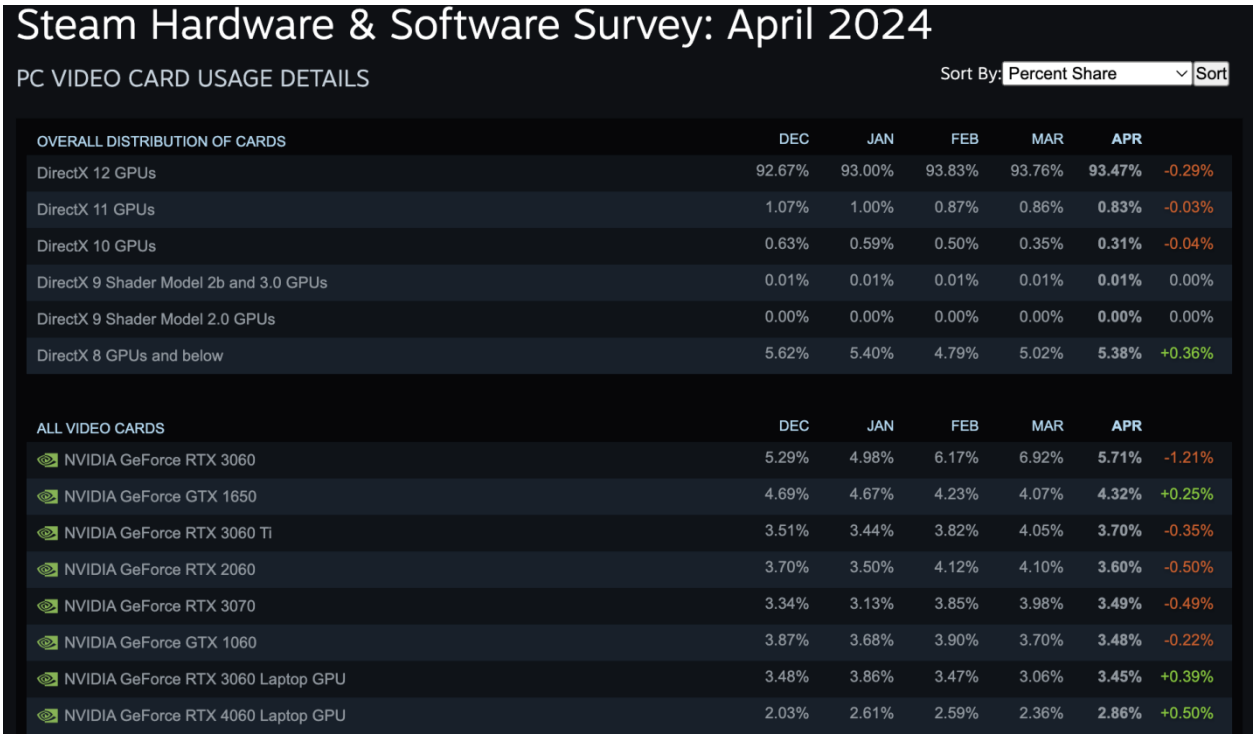

Figure 1. Steam Hardware & Software Survey: April 2024

Expanding on this premise, it's crucial to understand the technical and ethical implications of using such software. Cheating software, particularly those utilizing computer vision technology, harnesses the GPU for processing images and executing complex algorithms in real-time. This process requires substantial computational resources, which can limit its application to gamers with access to high-end graphics cards. This distinction creates an unequal playing field, where the financial barrier to entry for cheating increases with the sophistication of the cheating method. (Bird, 2024)

For example, a project on GitHub, a better original god. This project allows players to automate fishing and get rid of using the mouse to play boring mini-games to get fish. This project requires a higher configuration for the use of computer vision software to recognize and respond to images in real time (huiyadanli, 2024)

The model of the software itself also requires a lot of training to be used in the game. The testing is performed using a top-tier server equipped with dual Intel Xeon Platinum 8260L CPUs, each running at 2.4 GHz, which collectively offer a total of 48 cores. (Vasiliev et al., 2021) This shows that the performance of the computer used in the training model and inference model is beyond that of ordinary people. Of course, the cheating software development team can buy a powerful computer to train the model and distribute it to all players who need to use the cheating function in the game, but they still need a high-performance graphics card for the reasoning model. In summary, the economic cost of using computer vision (CV)-based cheating software is relatively expensive.

2.3. To What Extent Do Game Companies have Reasonable Corresponding Means to Deal with this Situation?

Cheating in the game is not all bad.A survey of 188 U.S. players regarding their beliefs, preferences, and experiences of cheating in single-player contexts revealed through mixed-methods analyses that, unlike in multiplayer settings, most players approve of cheating in single-player games. They do this to improve their mood, relieve stress, enhance flow, and exercise control over satisfying their psychological needs during gameplay.(Passmore et al., 2020). However, cheating in FPS games will cause discomfort to other players, which is a bad behavior.

Cheat tools can disrupt game balance, lead to unfair losses for certain players, tarnish the game's reputation, and result in financial losses for the developer. This cheating behavior negatively impacts the gaming industry. Despite proactive measures by many game developers to combat cheating, these methods have not always been effective. (Detection of a Novel Object-Detection-Based Cheat Tool for First-Person Shooter Games Using Machine Learning, 2023)

The behavior of hackers using cheating software in online multiplayer FPS games is incorrect, which will lead to the loss of some players or more players using cheating software to fight against hackers. This is not a normal game community environment, and the loss of players will affect the economic interests of game companies, so game companies need to prevent hackers from using cheating software. According to the mechanism of FPS games, detect whether a player has hurt other players. Now the method adopted by the game company is to upload the relevant information from the corresponding player client and submit it to the server for inspection. In this mode, cheating software can modify the uploaded information, cheat the server, and make the cheating software achieve its goal. So how to prevent cheating software? Here are several possible ways. First, upload all the files to the server for inspection. This method is effective and the files modified by the cheating software can be checked out. Valve Anti-Cheat software can detect cheating by hackers based on OPENGL software. Lehtonen, S. (2020). However, the current network rate cannot transmit complete data in real time, and the server may not have enough performance to check files in real time. The second is to check the software running in the background. This method can detect cheating software and prevent it from running. This method is better for memory-injected cheating software, but because computer vision (CV) cheating software does not modify the program file, but only performs image recognition and then moves the mouse(AbdElminaam et al., 2020), this method of detecting cheating software cannot work on computer vision (CV) cheating software. The third type: use the artificial intelligence detection program made by the game company. The purpose of any player using cheating software is to kill the enemy, so he needs to move the mouse at high speed and accurately. The mouse trajectory of the program is smoother and faster than that of the human mouse. (Kanervisto et al., 2023) By training artificial intelligence, the game company can detect the trajectory of mouse movement to analyze whether the player is using a cheating program.

There is also a feasible way to encrypt the files used for transmission so that the cheating software cannot intervene in the modification, or encrypting the transmission channel can also increase the possibility of cheating software intervention to a certain extent. Finally, it is a high-cost way: to influence the cheating software development team through legal means, making it impossible for them to continue to develop cheating programs. Continuous crackdowns can make the circulation of cheating software more difficult, thus reducing the probability of hackers using cheating programs.

Finally, game companies can use the player community to reduce the generation of cheating players. We observed that being labeled as a cheater carries a social penalty: individuals lose friends immediately after the cheating label is publicly assigned(Blackburn et al., 2014). Game companies can choose some experienced players as game behavior supervisors. The game company trains artificial intelligence models to screen some highly suspected players as targets. At the same time, they record the game process of these players and give them to the supervisor. They can check out some unreasonable behaviors by observing the video and select cheating players.

3. CONCLUSION

In this article, the article proves that artificial intelligence has a greater impact on fps games, especially the negative impact. Among them, the article proves that the artificial intelligence image recognition system is better than the traditional memory injection cheating software. At the same time, although artificial intelligence image recognition cheating software is very powerful, the cost of use also limits its abuse. Finally, game companies can also use artificial intelligence to limit cheating programs, which reflects both sides of artificial intelligence. Artificial intelligence image recognition

should be used in more effective scenarios rather than as a tool to destroy the player's play environment.

REFERENCES

[1] AbdElminaam, D. S., Almansori, A. M., Taha, M., & Badr, E. (2020). A deep facial recognition system using computational intelligent algorithms. PLOS ONE, 15(12), e0242269. https://doi.org/10.1371/journal.pone.0242269

[2] Slack. (n.d.). GitHub - slack2450/csgo-dma-overlay: A basic CS: GO ESP utilising DMA and HDMI-Overlay. GitHub. https://github.com/slack2450/csgo-dma-overlay

[3] GAN-Aimbots: Using machine learning for cheating in first person shooters. (2023, December 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/9774028/references#references

[4] Vasiliev, E., Кустикова, В., Volokitin, V., Kozinov, E., & Meyerov, I. B. (2021). Performance analysis of deep learning inference in convolutional neural networks on Intel Cascade Lake CPUs. In Communications in computer and information science (pp. 346–360). https://doi.org/10.1007/978-3-030-78759-2_29

[5] Lehtonen, S. (2020). Comparative study of anti-cheat methods in video games. University of Helsinki, Faculty of Science.

[6] Detection of a novel Object-Detection-Based cheat tool for First-Person shooter games using machine learning. (2023, May 23). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/10197816

[7] Detecting passive cheats in online games via Performance-Skillfulness inconsistency. (2017, June 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/8023159

[8] Blackburn, J., Kourtellis, N., Skvoretz, J., Ripeanu, M., & Iamnitchi, A. (2014). Cheating in online games. ACM Transactions on Internet Technology, 13(3), 1–25. https://doi.org/10.1145/2602570

[9] Kim, J. E., & Tsvetkova, M. (2021). Cheating in online gaming spreads through observation and victimization. Network Science, 9(4), 425–442. https://doi.org/10.1017/nws.2021.19

[10] Passmore, C. J., Miller, M. K., Liu, J., Phillips, C. J., & Mandryk, R. L. (2020). A Cheating Mood: The Emotional and Psychological Benefits of Cheating in Single-Player Games. Digital Library. https://doi.org/10.1145/3410404.3414252