

AI cheating versus AI anti-cheating: A technological battle in game

Mingtao Chen

School of Computing Science, Zhujiang College, South China Agricultural University, Guangzhou, Guangdong, 510900, China

waynechen2731@foxmail.com

Abstract. Before AI (Artificial Intelligence) became popular, the way people cheated in video games was easily detected. However, everything changed when some cheaters found that AI could be used in cheating. When AI cheating replaces traditional cheating and becomes a popular cheating method, AI anti-cheating rises to the occasion. This paper presents the difference between AI cheating and traditional cheating, how AI cheating works use the YOLO (you only look once) , a model to achieve object detection as an example), and the differences between normal anti-cheating systems and AI anti-cheating. Through Python, the author built the basic cheating system and comprehended how the cheating system works by image recognition. In conclusion, building the anti-cheating system is harder than building the cheating system, because the cost of resources and the engineering difficulty are more and harder than the cheating system. That is the reason why the game company still uses the traditional anti-cheating system in now a day.

Keywords: AI Cheating, AI Anti-Cheating, Artificial Intelligence (AI).

1. Introduction

While video games become popular, they soon become an area where can make hundreds of millions of dollars of profit each year such as establishing professional competitions; and buying and selling game items. However, cheating is always a problem in video games [1]. Some cheaters are trying to get higher achievements in the game, and outside of the game, they will earn money from direct transactions with players, such as Powerleveler(Completing things like upgrades, quests, playing for money, etc. for other players who pay for it to earn income.)Cheating allows them to do it more efficiently. Cheating is always an indelible problem in video games, and the rapid development of AI(Artificial Intelligence) makes it harder for anti-cheating systems to identify the real cheaters. There are many ways to cheat[2] and Anti-cheating systems cannot be updated in time which make the cheater still active in the game, that is the reason why the decreasing of number of people playing video game and the company's reputation was damaged. Especially in the fps game, Because of the fps(First-person shooting game) game mechanics, there is more uncertainty than other type of game like Moba (Short for Multiplayer Online Battle Arena, also known as the action real-time strategy game, such as Dota2, League of Legends) game, it can use one bullet to make the kill, so that a single cheating performance in a fps game doesn't feel like cheating, but may be considered a subconscious action. An experienced cheater usually does not use obvious cheats to the point where the anti-cheat

system is unable to recognize that the player is cheating and a manual review is required but while AI is used in cheating, a manual review becomes useless except for the reviewer is the experienced player. Nowadays, when cheaters find AI can be used in cheating, cheating becomes harder to detect. This situation leads to the thinking of an AI anti-cheating system. By reading the relevant literature[3], some AI anti-cheating systems experiments that were successfully detected cheaters with close to 100%. This is an amazing achievement that can eliminate almost all cheaters, but on the other hand, when cheaters start to create a new cheating system by AI, AI anti-cheating system is still in their infancy, but AI cheating has been developed to approximate real people who are playing in the game.

can this accuracy be maintained? That aroused my curiosity, about how should AI anti-cheating systems be improved and how to work in detecting emerging cheating (such as AI cheating). The AI anti-cheating system is not practical, so it can only be verified through papers and my way.

2. Traditional cheating and AI cheating

2.1. Traditional cheating

Most of the cheats are well known in the development of the game[4], but the way to cheat is still updating, Identifying new cheating methods is a necessary behavior for anti-cheating systems. The cheat form most used by cheaters at the moment is hardware cheats which is called DMA(Direct Memory Access) cheating. This is a cheat that is widely used in fps games nowadays, it has almost the same way as other cheats such as predicting the enemy's position in advance, and having the same weapon but with significantly higher weapon stats than others. but it has the advantage of not being gcukn{" fgvgvgf0" FOC0u" hwnn" pcog" ku" Fktgev" Ogoqt{" Ceeguu." yjkej" wugu" vjg" REKG(peripheral component interconnect express) devices to read and write physical memory directly and then bypass the operating system so that it can read and write memory operations in the case of the target machine without any code. This type of cheating usually involves two computers, one with only the game content and the other with a cheating system. It is difficult for anti-cheating systems to detect this cheating, which can only be detected through manual review.

2.2. AI cheating

Most of the AI cheats are pretty much the same. That is, they are all recognized by the image and then the mouse cursor is moved to the desired position. Use the open-source target recognition program YOLO(you only look once) as an example. YOLO is an object detector in a machine learning algorithm, commonly known as You Only Look Once, whose purpose is to detect objects in a given image and locate their positions. The YOLO algorithm is mainly implemented through a CNN(Convolutional Neural Network) neural network, which performs a forward transfer calculation on the entire image, generating information such as object category, position, bounding box, etc. Compared with other object detection algorithms, YOLO's main characteristics are its fast speed and accuracy, making it one of the preferred algorithms for many computer vision applications. As Yolo continues to be updated, the cheating programs based on it become more powerful in terms of image responsiveness and recognition[5]. 6 steps need to be moved before the YOLO can be used: Data preparation, Data preprocessing, Model construction, Model training, Evaluation, and Model deployment. After completing the base of image recognition, move into applying it in practice. After training the model to recognize the name of the object in the image and to mark the position of the object using a box, the distance, and orientation of the mouse to be moved can be accurately calculated. The specific calculation process is as follows: in the recognition process, the name of the returned items can be stored in an array, and each item in this array can find the corresponding object position in another multivariate array of returned positions, and then calculate the distance that the cursor needs to be moved by this positional information, and through the calculation, we can get the center position of the character and then compare it with the center of the screen, that is, we can get the distance that the cursor needs to be moved(The position information obtained is the upper and lower edges, left and right edges of the marked box.).After the completion of the analysis, the external video capture card

records the game output screen on computer A and then immediately transfers to another computer B, carries out the above content, and then sends it to the controller to complete the computer A mouse movement

2.3. *The difference between AI and traditional cheating*

As mentioned above, traditional cheats are more about altering the game's stats and obtaining stats that are not available to normal players. The differences between traditional and AI cheating can be directly categorized in two ways: Firstly, as mentioned above, traditional cheating is more about changing the game's stats and gaining access to stats that are not available to normal players. This is much easier to detect than AI cheating, especially during manual review. And AI cheating is more like a real player who never misses the shot. In most FPS games, guns will have recoil. Traditional cheats usually modify the recoil stats to ensure that every bullet will land on a point. AI cheats only aim at the opponent, but do not control the recoil, thus looking more like a normal player. This is one of the reasons why AI cheats are so difficult to detect, even when manually checked! In addition, the cost of AI cheating as well as traditional cheating methods is also very different. Two computers used in the YOLO application for AI cheats mentioned above can be optimized as a single computer, in case your computer configuration is good enough. The DMA cheat mentioned above is currently the most used and hardest to detect of the traditional cheats. DMA is a special circuit board that plugs into a PCI Express and reads data from the CPU, passes it through DMA to another computer, and runs the cheats program on that computer, the computer that plays the game doesn't run any cheats program, unlike memory-reading cheats program that can be detected. This means that when you use DMA cheats, you need to have two computers with advanced configurations, This means that your cost of cheating is much higher than if you were using the AI cheating. In this way, AI cheating will gradually replace traditional cheating methods.

3. Traditional anti-cheating and AI anti-cheating system

3.1. *Traditional anti-cheating system*

There are several better-known anti-cheating systems on the market (Games using this anti-cheat system are shown in parentheses): BattleEye (Rainbow 6), VAC (cs: go), Vanguard (Valorant), Easy Anti-Cheat (APEX LEGEND). Of these 4 anti-cheating systems, VAC and Vanguard are the best-rated. In most anti-cheat systems, the anti-cheat methods are basically in these three categories [6].

Scan Run Environment: An anti-cheating system such as BattleEye is somewhat similar to antivirus software - scanning the running environment before the game starts to ensure sufficient security while protecting the game program from external modifications during runtime to prevent external programs from running, and ensuring that the entire data is encrypted and sent to the corresponding server. If the data is interrupted, the player's session will be terminated.

Manual review: For example, in the VAC "monitoring system", staff/volunteers (usually reputable players) are allowed to watch the first-person screen to determine whether the player is a cheat. This is the best way to determine whether a player has cheated, provided that the observer has a certain level of experience and gaming skills.

Hardware ban and real name registration-based games: Record the serial codes, such as the motherboard, CPU, network card MAC code, and IP address of the player's machine, and upload them to the development team's dedicated database for recording. If the anti-cheating system discovers the use of illegal plugins or third-party cheating software for cheating, the anti-cheating system will ban the account and blacklist the sequence code and IP address in the database. In this way, even if banned players log in to different accounts on the same computer, they will be banned. Among the anti-cheat systems mentioned above, the paper highlights VAC and VANGUARD.

3.1.1. VAC. VAC is known as Valve Anti-Cheat, an anti-cheat solution developed by Wilford, and one of the components of the Steam game development platform. VAC. Through the paper [7], the design

of VAC is confidential which makes sure that cheaters will not learn the principle of the anti-cheating system through insiders' leakage to make corresponding cheating procedures. However, through the analysis of some cheaters, the VAC system is a system that can automatically detect and update the feature code library and manually add feature codes. And what are feature codes? What are the feature codes? A signature is a sequence that the compiler generates from the code, and different combinations of code have different sequences. But of course, VAC doesn't detect all the sequences, because it's easy to avoid a ban that way (just change a random code sequence and it changes). After it confirms that something in memory is a cheat, it will randomly intercept a sequence of features and update it to the feature code database, and then as soon as it detects the same sequence from any PC, it will be blocked by VAC. Even with such a stringent anti-cheating system, there are still some cheating programs and programs that bypass the system. The regulation system is to ban the cheater through manual review, and the regulators are composed of ordinary players who have had 150 rank match win-wins in a single season. When a player receives 11 valid reports within 24 hours, then after the eleventh report, the match demo will be distributed to at least 8 and as many as 11 supervisors to determine whether or not it is cheating. Regulators will review the entire match demo under suspicion, and when a majority of Regulators determine that a player has cheated, the player will receive a Regulatory Ban.

3.1.2. *Vanguard*. Through the internet[8], Vanguard is an anti-cheat system developed by Riot itself, the code part is through Riot's development of the packman, the basic principle for the unimportant code variant insertion, the key code virtualization, increasing the difficulty of the plug-in maker to analyze the anti-cheat. The core strategy of Vanguard is a faceit-like boot load driver (boot type) that stops all subsequent problematic drivers from loading. Because he needs to make sure he loads it during the boot phase of the system, he asks you to reboot your computer after the first installation. If people forcefully modify its driver code to make it support dynamic loading, it will trigger an account ban. Specific Vanguard components are known through media interviews with Paul Chamberlain, the person in charge of security and anti-cheating at RIOT[9], Vanguard consists of two main components: a traditional scanning service that starts when the game is running, and a device driver that is loaded at system startup. Even if you don't play Valorant, the driver will always be running on your computer. The driver itself does not perform any scanning or communication with the network or anything similar. It ensures that the system is not compromised or tampered with from the time the computer starts up until the game begins. It does this by booting up before any cheat files are loaded on the system. Then, when new drivers or modules are loaded on the computer, it checks them for security vulnerabilities. If they do, they are not allowed to load.

3.2. *AI anti-cheating system*

There are no concrete examples of AI (Artificial Intelligence) anti-cheat systems in games because they are not fully widespread. The AI anti-cheat system is more of a future outlook. After reading through the papers, The author found out that there are still people working on the AI anti-cheat system [10-12]. The author will analyze the flaws and strengths of AI anti-cheating systems

3.2.1. *Advantage of AI anti-cheating system*. Automation: The AI anti-cheating system can automatically identify, monitor, and handle cheating behaviors without the need for manual updates or configuration of rules. It can continuously learn and adapt new cheating methods, improve detection accuracy, and reduce false alarms. Real-time: The AI anti-cheating system can monitor the game environment and player behavior in real time, and detect and respond to cheating behaviors promptly. In contrast, traditional anti-cheating software may require a long period of development and updates to adapt to new cheating methods and behaviors. Adaptability: The AI anti-cheating system utilizes technologies such as machine learning and reinforcement learning to analyze and identify new cheating patterns in real-time, and quickly adjust to emerging cheating methods. Traditional

anti-cheating software may need to manually update rules to cope with new cheating behaviors, resulting in slower response times.

3.2.2. Drawback of AI anti-cheating system. The Cost Constraint: Compared with traditional anti-cheating technologies, AI anti-cheating technology has certain technical barriers and application barriers. In most current game anti-cheating systems, to pursue the goal of simplicity and ease of use, mature technologies are usually used to save costs. The AI anti-cheating system requires more advanced and sensitive technologies and algorithms to ensure the accuracy and judgment of the anti-cheating system, which requires higher investment and technological accumulation. The AI anti-cheating system also requires a large data and user information for training and testing: game companies invest a lot of cost and effort, while also complying with strict privacy protection regulations. This may lead some gaming companies to wait and explore cautiously, rather than quickly applying AI anti-cheating technology. Initial AI anti-cheat systems may have a high rate of false positives: Since AI anti-cheating systems require a large training set for iterative updates in the same way as AI cheating. The difficulty of collecting the training set required by the AI anti-cheating system is significantly greater than that of AI cheating because it requires manual judgment to determine whether the player is cheating before putting it into training, however, the manual judgment can be misjudged, which may result in the completion of the training of the AI anti-cheating system will be blocked by the normal players, which will lead to loss of the number of players and loss of the company's reputation. Therefore, most of the companies that develop anti-cheat systems may not have embarked on the research and development of AI anti-cheat systems.

3.3. The Future of AI Anti-Cheating Systems

Strengthening user reporting systems: AI technology can improve user reporting systems, and automate the processing and analysis of user cheating reports. The system can accurately distinguish between real cheating behaviors and false positives through automated evaluation and verification, thus making it faster to handle and respond to cheating behaviors.

Clusters can collaborate: AI anti-cheating systems can adopt a cluster intelligent collaboration approach, where multiple anti-cheating models can learn and work together to improve detection accuracy and effectiveness. This system can better cope with complex and team cheating behaviors, and improve the game's anti-cheating ability

Reinforcement learning confrontation: Use reinforcement learning technology to build an anti-cheating system for games. The system continuously improves its recognition ability by engaging in adversarial learning with cheaters, effectively identifying and preventing new types of cheating behavior.

4. Conclusion

This article describes traditional and AI cheating as well as anti-cheating systems. There are many types of traditional cheats, and this article focuses on the cheats through DMA(Direct Memory Access), while AI cheats are AI cheats based on YOLO(you only look once), which can be widely used in addition to weekday recognition and can also be used in-game cheats. As for the anti-cheat system, the traditional anti-cheat system takes VAC and Vanguard as examples to illustrate the characteristics of the traditional anti-cheat system. However, due to the unequal relationship between cheating and anti-cheating, it is easier to update the cheating program, while the anti-cheating needs to be updated after the cheating program program has been updated, and there is a delay. Fortunately, with the popularity of AI, perhaps shortly, AI anti-cheat systems can replace the traditional anti-cheat system, to give the game a better environment. This paper has many shortcomings. The author fklfpøv"ngctp" enough programs about AI anti-cheating systems and practice them. In the next step, It is necessary to analyze how to popularize AI anti-cheating systems and find ways to improve the shortcomings.

References

- [1] Bryan van de Ven. Cheating and anti-ejgcv"u{uvgo"cevkqp"ko rcevuwugt"gzrgtkgpeg0"Dcejgnqtøu" Thesis Computing Science. 2023. 19-23
- [2] Jeff Yan and Brian Randell . A Systematic Classification of Cheating in Online Games. Publication History. 2005. 2-4
- [3] José Pedro Pinto, André F. F. Almeida and Paulo Novais . Deep learning and multivariate time series for cheat detection in video games. Springer Nature. 2021
- [5] Peter Laurens; Richard F. Paige; Phillip J. Brooke; Howard Chivers. A Novel Approach to the Detection of Cheating in Multiplayer Online Games. IEEE. 2007
- [6] PeiyuanJiang,DajiErgu,FangyaoLiu,YingCai and BoMa . A Review of Yolo Algorithm Developments. Elsevier. 2022
- [7] Tqpmckpgp." Yctcp{qq"0"Rtgxgpkqp" xu" fgvgvkvqp" kp" qpnkpg" icog" ejgcvkpi0"Dcejgnqtøu" Vjgukuo" 2021
- [8] Salman Khalifa . Machine Learning and Anti Cheating in FPS Games. researchgate. 2016.<https://baijiahao.baidu.com/s?id=1767593419798574769&wfr=spider&for=pc>
- [9] How exactly does VALORANT's anti-cheat system, Vanguard, work? (2023). <http://www.imbatv.cn/article/29021>
- [10] Sparsh Bajaj. Detect Cheater in Online Gaming using AI. Thesis (Masters). 2022
- [11] Jianrong Tao, Yu Xiong, Shiwei Zhao, Yuhong Xu, Jianshi Lin, Runze Wu, Changjie Fan . XAI-Driven Explainable Multi-view Game Cheating Detection . IEEE. 2020
- [12] Otavio Barcelos Gaspareto;Dante Augusto Couto Barone;André Marcelo Schneider . Neural Networks Applied to Speed Cheating Detection in Online Computer Games . IEEE. 2008