Proceedings of the 2023 International Conference on Machine Learning and Automation
DOI: 10.54254/2755-2721/43/20230844

# Cryptography and DRM: A study of digital copyright protection in the gaming industry

**Yixiang Shen**

Department of Electrical, Information and Physics Engineering, Tohoku University, Sendai, Japan

hirosawa.ishou.r6@dc.tohoku.ac.jp

**Abstract.** This paper explores the role of cryptography and encryption technology in developing digital rights management (DRM) in the gaming industry. DRM aims to protect the rights of creators by preventing unauthorized copying and distribution of digital media. Cryptography plays a crucial role in DRM, ensuring the privacy, authenticity, and integrity of data. The early stages of game DRM involved physical disc methods, such as unique disc characteristics and online activation. However, these methods faced challenges such as compatibility issues and unauthorized copying. Modern DRM technologies combine advanced encryption techniques with account-binding mechanisms, requiring users to activate and access game content on specific accounts. Cryptography plays a key role in DRM by encrypting game data into unreadable formats, ensuring that only users with valid decryption keys can access the content, and ensuring secure distribution and consumption of digital content. The paper also discusses third-party DRM technologies, such as Denuvo, which employ strong encryption and obfuscation methods. However, third-party DRM may impact performance, inconvenience users, and lead to compatibility issues. The paper emphasizes the necessity of continually refining DRM technologies to balance copyright protection and consumer rights in the evolving gaming industry.

**Keywords:** DRM, cryptography, Gaming Industry, third-party DRM technologies.

## 1. Introduction

Digital Rights Management (DRM) has been a critical tool in the arsenal of game developers and publishers for safeguarding their intellectual property from piracy and unauthorized distribution. Since the early days of video game distribution, piracy has posed significant challenges, leading to the evolution of DRM technologies [1]. This paper explores the history of video game piracy, from its inception during the era of audio compact cassettes and optical discs to the modern challenges faced with sophisticated encryption technologies like Denuvo. It delves into the various problems associated with third-party DRM, including performance impact, inconvenience, and compatibility issues. Additionally, it examines alternative approaches to DRM and contemplates the future of DRM in the gaming industry. Despite its necessity and efforts to enhance its effectiveness, DRM continues to face challenges, including the availability of cracked versions of games and the inconvenience it sometimes imposes on legitimate users. The continuous evolution of technology and the ingenuity of hackers

DOI: 10.54254/2755-2721/43/20230844

necessitate a reevaluation of current DRM strategies and the exploration of alternative approaches to protect intellectual property while ensuring an optimal experience for legitimate users.

## 2. Early Stage

Video game piracy has been a challenge since the inception of the first video games that could be duplicated and either resold or freely shared, as was common in the early days of personal computers. Initially, video games were distributed on audio compact cassettes, which were incredibly easy to replicate due to the widespread availability of dual cassette players – all that was needed was a blank cassette. This ease of duplication led to many game publishers worldwide shutting down. To combat this, the industry invested significant effort in devising and implementing various technologies [2]. DRM was previously focused on security and encryption as tools to prevent illegal duplication. The content was locked and distributed only to authorized persons. In terms of rights management, this was a narrow implementation. Currently, DRM presents broader capabilities. It covers the description, identification, protection, trading, monitoring, and tracking of all rights usage forms over all types of content [3].

In the early days of gaming, optical discs were widely used. During the era of disc-based games, a common DRM method involved writing the game program and resource files onto the disc and utilizing the physical characteristics of the disc for verification. This could include employing special disc copy protection, disc verification, and encryption measures, among others.

One common DRM technique involved incorporating special physical features on the disc, such as intentional errors or unique patterns. These features were difficult to replicate accurately, making it challenging to create functional copies of the original disc. The game's program or resource files were often encrypted or encoded in a way that required these physical features for successful decryption. However, this technique has compatibility and disc damage problems. Because the presence of special physical features on the disc could cause compatibility problems with certain disc drives or players. Some users might experience difficulties in reading or running the game due to compatibility issues. Besides, Intentional errors or unique patterns on the disc could make it more susceptible to damage. Even minor scratches or wear on the disc could render it unreadable or cause errors during the decryption process, preventing legitimate users from accessing the game.

Additionally, disc-based DRM systems often require users to have the original disc inserted into their computer's optical drive while playing the game [4]. This was done to verify the authenticity of the disc and ensure that it hadn't been duplicated or illegally distributed. The game would check for specific indicators on the disc, such as hidden sectors or unique identifiers, to validate its legitimacy. Despite the DRM measures, determined individuals could find ways to bypass the disc-based authentication system and create unauthorized copies of the game.

Some games also employed additional measures like online activation or verification processes, where users had to enter unique serial numbers or connect to a server to authenticate their game copy. These methods helped prevent unauthorized use of the software and protected the rights of game developers and publishers. However, it did not prevent much copying, as within a few weeks, crackers can retool a working key generator for the game. Due to the various issues mentioned earlier, games required additional protection, leading manufacturers to turn to what is now considered modern DRM research.

## 3. Modern DRM Technology

Digital Rights Management uses various methods to fight piracy, which can be broadly classified into two categories: mechanisms based on cryptography and mechanisms based on watermarking. These include techniques such as encrypting content, using passwords, embedding watermarks, utilizing digital signatures, creating digital fingerprints, implementing copy detection systems, and managing payment systems [5]. DRM technology currently relies on 128-bit AES encryption, which is widely considered extremely difficult to crack using today's computer capabilities. Even if an encrypted file falls into the wrong hands, such as a rogue staff member at a distribution partner, the content remains

DOI: 10.54254/2755-2721/43/20230844

inaccessible. Without the necessary tools and information to decrypt or unscramble the file, it holds no value.

Cryptographic mechanisms protect rights by ensuring the security of content distribution. In this approach, digital content is always shared in an encrypted state, and only authorized users receive access rights from content providers. However, once the content is decrypted, it loses all copyright information, making it impossible for the provider to track its further distribution and replication. This is a copy control issue that DRM technology based on cryptography cannot resolve [6]. Additionally, implementing cryptographic methods is complicated, making it expensive and less compatible [7]. For DRM to function, users must possess media players that can recognize protected content and request the corresponding key to unlock it. Additionally, rights holders must operate a license server that responds to legitimate requests by providing the key required to reverse the encryption.

Considering offline DRM technology, it will be continuously scrutinized and exploited by warez groups, resulting in the development of replicas [8]. Modern DRM technologies, for the most part, require network authentication. A very common way of providing modern DRM service is online distribution like Steam, Games for Windows Live, Origin, and Uplay. They act as both retail services and DRM solutions. They provide a centralized marketplace where users can purchase and download games securely. These platforms require users to create accounts and install client software, which serves as a gateway to access and manage their game library. They have stacked DRM protection i.e., they use third-party DRMs like Denuvo and VMProtect along with their own DRM. Games are sold via the client and verified via servers, and the client runs in the background during gameplay.

## 4. Third-party DRM problems

Denuvo is one of the most popular third-party DRM technologies, known for its robust encryption and obfuscation techniques. The exact details of Denuvo's encryption algorithm are not publicly disclosed, as the company considers it a trade secret. However, it is known that Denuvo employs advanced encryption and obfuscation methods to safeguard game executables against tampering and reverse engineering [9]. A significant element of Denuvo's approach is using a virtual machine, which executes the game's code within a highly protected virtual environment. This virtual machine is heavily obfuscated, employing multiple layers of encryption and anti-debugging measures to deter hackers from analyzing or manipulating the code.

In addition to the virtual machine, Denuvo employs various obfuscation techniques like code splitting, making it challenging for hackers to comprehend the structure and flow of the game's code. It also incorporates anti-debugging measures such as memory scrambling to thwart attempts by hackers to attach debuggers and examine the game's behavior.

Although third-party DRM like Denuvo is considered one of the most effective anti-tampering solutions available, it does have some problems.

(1) Performance Impact: third-party DRM, including Denuvo, can introduce performance overhead to games. Users have reported decreased frame rates and longer loading times when DRM is present, which can negatively impact the gaming experience. For example, in 2017. a study by Overlord Gaming found that games using Denuvo had an average 15% reduction in frame rate and a 30% increase in loading times compared to the same games without Denuvo. The experiment conducted by J. Karthik, P. P. Amritha, and M. Sethumadhavan also revealed that there was an average of 8% increase in FPS, 32% decrease in loading time, and 60% decrease in .exe file size across the games with no DRM in comparison with the respective DRM-enabled run [10].

(2) Inconvenience: Indeed, some players have reported that they cannot launch Denuvo-protected games without an internet connection, which can be inconvenient for those who travel frequently or have unstable network connections. One implementation of Denuvo involves online verification, where the game needs to communicate with Denuvo servers during the startup process to validate its legitimacy. Without an internet connection, the verification process cannot be completed, resulting in the inability to launch the game. This can be particularly inconvenient for players who rely on offline gaming or find themselves in situations where an internet connection is not readily available.

DOI: 10.54254/2755-2721/43/20230844

For example, games like RedFall and SimCity require an internet connection even for single-player mode, further exacerbating the issue. Although these games primarily feature a solo gameplay experience, the necessity of an internet connection remains due to design choices made by the developers. This means that players who do not have a stable internet connection or frequently find themselves offline may encounter difficulties launching or playing these games. Consequently, the always-online requirement can pose a significant inconvenience for players, especially those who travel extensively or reside in areas with limited internet connectivity.

(3) Incompatibility: Denuvo itself does not have inherent compatibility problems. It is designed to be compatible with various hardware configurations and operating systems. However, compatibility issues can still arise due to various factors such as:

A) Hardware or software conflicts: Certain combinations of hardware components, drivers, or software applications can cause conflicts with Denuvo or the game using it. In such cases, the game may not run properly or may encounter errors.

B) System configurations: Some games with Denuvo may have specific system requirements that need to be met for proper compatibility. If your system does not meet these requirements, you may experience issues running the game.

C) Pirated copies: Denuvo is primarily designed to prevent piracy, and it can cause compatibility issues with unauthorized or cracked copies of games. These copies may have modified files or missing components, leading to errors or crashes.

When releasing new CPUs each year, it is possible for compatibility issues to arise with Denuvo-protected games. Denuvo, being an anti-tamper technology, relies on various underlying systems and hardware components to function properly. Therefore, changes in CPU architectures or technologies introduced by Intel or AMD may occasionally lead to compatibility problems with Denuvo [11,12]. For example, when Intel released the 12th generation CPU, there were tons of games that had compatibility issues.

### *4.1. Cracking and availability of pirated versions*

Despite robust protections, hackers and pirate groups have still found ways to crack Denuvo and other DRM protections. Once cracked, these games are often distributed illegally on torrent sites and other online platforms. This not only leads to financial losses for game developers and publishers but also poses legal risks for users downloading and playing pirated games. Hackers employ various techniques to bypass DRM protections, including reverse engineering, code modification, and emulation. Reverse engineering involves analyzing the game's code to understand its structure and behavior. This knowledge is then used to modify the code to bypass DRM checks or to create a key generator (keygen) that can generate valid activation keys. Emulation involves creating a software program that mimics the behavior of the DRM, tricking the game into believing that it is running on a legitimate system. The availability of cracked versions of games undermines the efforts of developers and publishers to protect their intellectual property. It can lead to financial losses, as users may choose to download pirated versions of games instead of purchasing them legally. Additionally, the development and distribution of cracked games are illegal and can pose legal risks for users who download and play them.

### *4.2. Future of DRM*

Despite the challenges associated with DRM, it is still considered a necessary tool for protecting intellectual property and ensuring fair compensation for developers and publishers. However, the effectiveness of current DRM solutions is being questioned, and there is a growing call for alternative approaches.

### *4.3. Alternative Approaches*

One alternative approach to DRM is adopting a subscription-based model, where users pay a monthly fee to access a library of games. This model has been successfully implemented by platforms like Xbox Game Pass and PlayStation Now. Another approach is to focus on providing additional value to

DOI: 10.54254/2755-2721/43/20230844

legitimate customers, such as exclusive content, updates, and support, which may not be available to users of pirated versions. Some developers and publishers have also adopted a DRM-free approach, relying on goodwill and the support of their community to combat piracy.

## 5. Conclusion

In conclusion, DRM has played a crucial role in protecting the intellectual property of game developers and publishers. However, its effectiveness is being challenged by the availability of cracked versions of games and the inconvenience it causes to legitimate users. Alternative approaches, such as subscription-based models and providing additional value to legitimate customers, are being explored, but they come with challenges. As technology evolves, it will be interesting to see how the landscape of DRM changes and how developers and publishers adapt to protect their intellectual property and provide the best experience for their customers.

## References

[1] E. Becker, W. Buhse, D. Gunnewig, and N. Rump, (2003)."DRM as an Interlocking Challenge for Different Scientific Disciplines: Introduction," in Proceeding of Digital Rights Management: Technological, Economic, Legal and Political Aspect (LNCS 2770), pp. 1-2

[2] Tsotsorin, Maxim, (2012).Piracy and Video Games: Is There a Light at the End of the Tunnel?

[3] R. Iannella, (2001). "Digital Rights Management (DRM) Architectures," D-Lib Magazine, vol. 7 pp. 1-15.

[4] Pcgamingwiki.com.(nd).Digital rights management (DRM). https://www.pcgamingwiki.com/wiki/Digital_rights_management_(DRM)

[5] M. Fetscherin and M. Schmid, (2003)." Comparing the Usage of Digital Rights Management Systems in the Music, Film and Print Industry," in 5th International Conference on Electronic Commerce, pp. 316-325.

[6] F. A. P. Petitcolas, (2003). "Components of DRM Systems: Digital Watermarking," in Proceeding of Digital Rights Management: Technological, Economic, Legal and Political Aspect (LNCS 2770), pp. 81-92.

[7] Y. Cheng, Q. Liu, X. Zhu, C. Zhao, and S. Li, (2011)."Research on Digital Content Protection Technology for Video and Audio Based on FFmpeg," International Journal of Advancements in Computing Technology, vol. 3, pp. 9-17.

[8] C. Cortner, "The Warez Scene," 2008.

[9] E2encrypted.com. (2023). How Denuvo encryption (D encryption) works. https://www.e2encrypted.com/posts/how-denuvo-encryption-works/

[10] J. Karthik, P. P. Amritha and M. Sethumadhavan, (2020)"Video Game DRM: Analysis and Paradigm Solution," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, pp. 1-4, doi: 10.1109/ICCCNT49239.2020.9225560.

[11] Andy Brown. (2021). Denuvo causes "the occasional incompatible game" with Alder Lake CPUs. https://www.nme.com/news/gaming-news/denuvo-causes-the-occasional-incompatible-game-with-alder-lake-cpus-3088448

[12] Michael Crider.(2022). Intel fixes the game DRM issue affecting 12th-gen Intel CPUs. https://www.pcworld.com/article/550267/denuvo-drm-crashing-dozens-of-games-on-12th-gen-intel-cpus.html