Movie Piracy Deterrence Using Infrared Transmitters and Cryptography Techniques

Authors

Tashwin J, ***Dept of CSE, Don Bosco Institute of Technology***

Champa C H, ***Dept of CSE, Don Bosco Institute of Technology, champa.ch@dbit.co.in***

Ravi Tejas R, ***Dept of CSE, Don Bosco Institute of Technology***

Vinay S, ***Dept of CSE, Don Bosco Institute of Technology***

Varshitha R, ***Dept of CSE, Don Bosco Institute of Technology***

Abstract

Movie piracy is a major concern for the film industry, contributing to substantial financial losses. Traditional deterrents like DRM and watermarking are limited in their real-time effectiveness. This paper reviews an innovative approach that integrates infrared (IR) interference through cryptographic algorithms like SM4. The system disrupts unauthorized recordings using near-infrared light, invisible to viewers but detectable by camera sensors. Additionally, authentication data is embedded into video frames using a modulo operator-based cryptographic method. The system triggers alerts through GSM and GPS modules for real-time notification. This hybrid approach offers both prevention and traceability, enhancing piracy deterrence in cinemas.

Keywords

Infrared (IR) Interference, Digital Video Cryptography, Movie Piracy Prevention, Modulo Operator Embedding, LSB Watermarking, Camera Signal Disruption, GSM-GPS Alert System, Anti-Piracy Technology, Multimedia Security, Real-Time Piracy Detection

Introduction

Piracy in the film industry is a critical issue that undermines the creative and financial investments made by filmmakers, distributors, and production companies. With the increasing accessibility of high-resolution recording devices, individuals are capable of discreetly capturing entire films during cinema screenings. These unauthorized copies are often uploaded to illegal streaming platforms or sold on physical media, impacting box office revenues, distributor agreements, and intellectual property rights enforcement. The limitations of conventional anti-piracy methods such as human surveillance, static warning signs, and watermarking demand the development of proactive and intelligent deterrent systems. In response, this paper reviews and synthesizes the design and effectiveness of a **dual layered anti-piracy system** comprising **infrared-based recording disruption** and **modulo operator-based steganographic encoding**.

Cinema remains a key form of entertainment, supported by substantial investments from filmmakers and production houses. However, film piracy has emerged as a major threat to the industry's financial stability. Unauthorized recordings of movies during theatrical screenings typically captured using concealed high-resolution cameras are often distributed illegally through online platforms and physical media. This practice results in significant revenue losses, disrupts distribution and licensing agreements, and undermines intellectual property enforcement. Furthermore, it discourages creative innovation by diminishing the returns on investment, ultimately affecting the quality and sustainability of future film productions.

This project presents a system designed to combat movie piracy in theaters by targeting digital camcorders. It works by sending out infrared (IR) signals towards the audience, which disrupt the recording capabilities of silicon-CCD based cameras. The system detects the presence of a camera by analyzing images to locate the lens. Once found, a beam of IR light is directed at it, causing overexposure that significantly degrades the recorded video, making it unsuitable for unauthorized distribution. Importantly, this method does not interfere with the normal viewing experience or harm the device or the person using it. Such a system could be effectively used to prevent illegal recording and content theft in cinemas and similar venues.

Literature Review

[1] Kalaimathi et al. (2024) introduced an automated IR transmission system combined with steganographic embedding for securing movie playback. Their work emphasized a real-time, non-intrusive solution that degrades the quality of camcorder-recorded content while maintaining an uninterrupted experience for cinema viewers. The integration of steganography ensures traceability of pirated copies, enabling forensic backtracking to the original source or theater

[2] Fouzar et al. (2023) Fouzar et al. proposed a multikey hybrid encryption technique for secure video communication over mobile platforms. The system segments video into chunks, encrypting each with dynamically generated AES keys derived from RSA and ECC-based equations. Implemented on Android, the approach achieved low encryption latency (≈1s/MB) and supported real-time playback, ensuring secure and efficient mobile video streaming.

[3] Narayanaswamy et al. proposed a forensic watermarking framework to detect camcorder-based piracy. Their research outlined methods to embed identifiable information within movie frames, which can later be extracted for legal validation and source tracking. This proactive strategy supports anti-piracy enforcement by offering tamper-resistant evidence present within the visual stream.

[4] Mareen et al**.** presented a camcording-resistant backup system that employs a secondary watermarking signal, their study explored a resilient watermarking layer designed to survive various forms of compression and re-encoding that pirated content typically undergoes. This approach provides enhanced robustness in hostile environments where traditional watermarking fails.

[5] Rani et al**.** explored deep learning and similarity-based algorithms to detect piracy in both movies and OTT content. Their methodology combined neural networks with visual pattern recognition to identify duplicated or altered content, thus providing a post-distribution surveillance mechanism. Although primarily aimed at OTT services, the core techniques are adaptable to cinema-based piracy scenarios.

[6] Nanditha L. et al. introduced a model to prevent unauthorized video recordings by combining IR-based interference with digital watermarking. Their research utilized LSB steganography to embed identifying information within video frames, while simultaneously using IR LEDs to distort footage captured by hidden cameras.

[7] Chethanya K. et al. proposed an automated anti-piracy system using IR LED technology to identify and block unauthorized recordings in real time. Their system included relay-based control mechanisms and user authentication features to improve theater-level security and ease of integration.

[8] A.M. Prasanna Kumar and Bharathi Gururaj emphasized the role of IR transmission in preventing camcorder piracy and integrating watermarking to trace the origin of leaked content. Their work demonstrated a proof-of-

concept setup for cinema halls using microcontroller-based coordination between sensors and communication modules.

[9] Sheeja Augustin et al. developed a content-tracking approach using unique identifiers embedded within video streams. These identifiers were extracted from leaked video content to pinpoint piracy sources, facilitating forensic tracking.

[10] BVV Rajesh Kumar et al. (2021) proposed an automated anti-piracy screen recording system aimed at mitigating illegal in-theater recordings. The study focused on real-time detection and interference using embedded hardware, integrating sensors and alert mechanisms to identify unauthorized recording devices. The system design emphasized automation, minimizing the need for human surveillance. Their evaluation highlighted reduced success rates of illicit recording attempts in controlled environments, suggesting the potential for broader deployment in commercial cinemas.

[11] Chandana P S et al. (2020**)**. developed a dual-layered anti-piracy framework incorporating an IR transmitter screen with steganography techniques. The IR system interferes with camcorder sensors without affecting human vision, thereby degrading the quality of pirated footage. Concurrently, steganographic encoding embeds metadata such as time, location, and operator identity into video frames. The system was tested in simulated theater conditions and was found effective in both deterring piracy and enabling the forensic tracing of leaks

[12] Dr. Venkata Kishore Kumar Rejeti et al. (2020) This study focused on practical approaches to preventing movie piracy using a combination of real-time monitoring and digital watermarking. The authors designed a prototype that detects recording devices via reflective sensors and responds by either alerting staff or degrading the display content. The approach was non-invasive and relied on embedded control circuits. Although the paper did not provide statistical analysis, effectiveness was measured by a reduction in successful recording attempts during test runs.

[13] B.P. Arjun et al. (2020) introduced a movie piracy tracking system based on video steganography. The approach allowed embedding of invisible yet retrievable tracking data within movie frames. The project used spatial domain embedding techniques to avoid detection or distortion by common video editing tools. The study was limited to a lab-scale environment, where the embedded data was consistently retrievable, confirming the robustness of the technique for forensic tracing.

[14] Sanju D J et al. (2020) presented an automated infrared transmission system for movie piracy prevention. Their design focused on a modular IR emitter setup installed around the cinema screen, creating a non-visible interference pattern that affects camera sensors. The system was built to operate automatically based on scheduled playback and audience detection. Prototype evaluations in mock theater setups showed significant degradation in camcorder recordings while maintaining viewer safety and visual comfort.

[15] Divya Rani et al. (2020) developed a movie piracy tracking system aimed at identifying the origin of pirated content using watermarking and video steganography. Their method embedded metadata within the video content using frame-based techniques. The system was evaluated for resilience against video compression and format conversion, and the data was successfully retrieved post-processing, validating its utility for piracy source identification. The study did not that have an extensive statistical analysis but demonstrated consistent success across multiple test scenarios.

Comparative Analysis

Earlier approaches to securing digital video content have relied on advanced cryptographic methods that combine RSA, ECC (Elliptic Curve Cryptography), and AES (Advanced Encryption Standard). These systems generate a distinct encryption key for each video segment, often derived from hardware-level identifiers such as the MAC address. This dynamic key generation approach not only improves the security of the transmission but also avoids the vulnerabilities associated with conventional key exchange methods. Such hybrid encryption mechanisms have proven effective in environments where maintaining data confidentiality and integrity is essential.

Another stream of research has focused on preventing in-theater piracy by disrupting the ability of cameras to record high-quality footage. Systems designed under this concept use infrared light sources aimed toward the audience, specifically targeting camcorders with CCD sensors. These IR emissions, though invisible to the human eye, cause distortion or overexposure in the captured footage. To enhance protection, some models incorporate steganographic techniques to insert traceable information into the video content and use RFID tags for authenticating playback devices. Integration with IoT technology allows for real-time detection of unauthorized recording activity and supports automated countermeasures.

The system proposed in this project offers a streamlined and efficient solution. It employs an Arduino microcontroller to control infrared LEDs arranged around the cinema screen. These LEDs emit IR light that interferes with the image sensors in recording devices, effectively rendering the footage unusable while leaving the viewer's experience unchanged. Access to the control unit is restricted via password protection, and current amplification is managed using drivers and relays. Furthermore, a Python-based steganography tool is used to embed invisible identification data within the video, allowing for content tracking. This dual-layered approach combining physical camera interference with digital watermarking provides a practical, low-cost alternative to more complex anti-piracy system

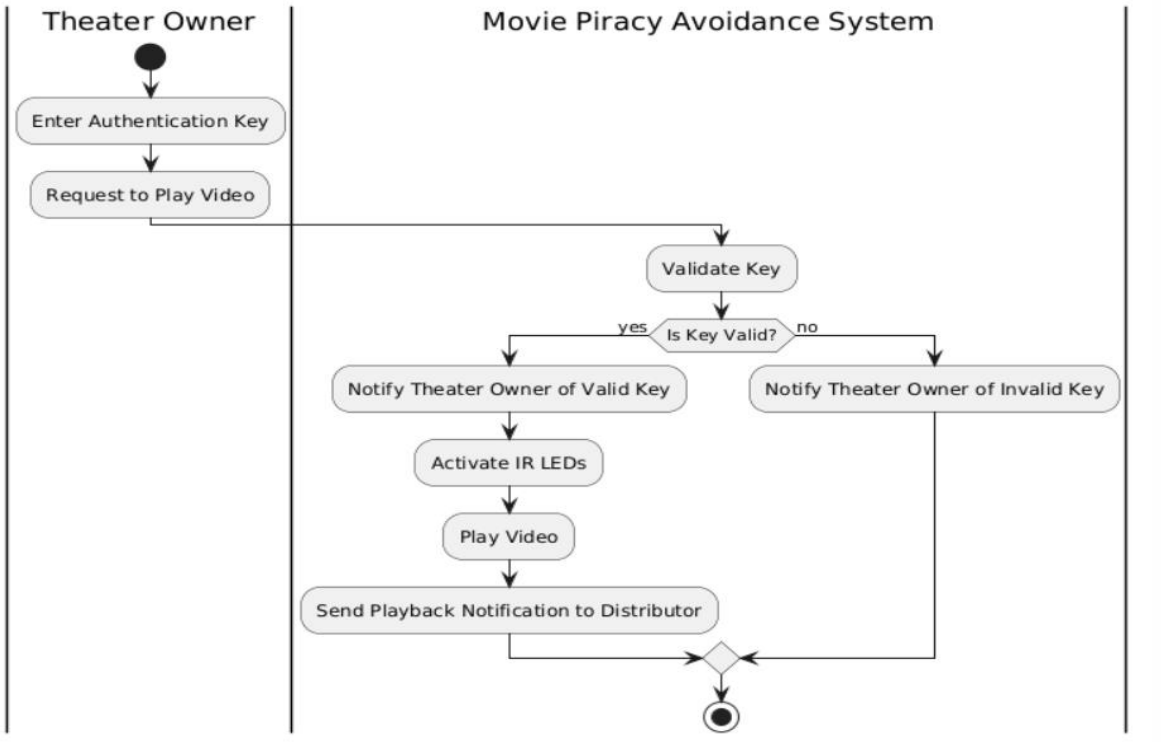


Fig : Block diagram representing working of piracy prevention system

Results/Discussion

Illegal movie recording in theatres is a major piracy issue causing financial losses. Traditional methods like DRM and watermarking are not always efficient against unauthorized recordings. Recent approaches use infrared (IR) light, invisible to humans but disruptive to many cameras, to prevent recording without disturbing viewers. Video encryption hides secret data within video frames, enhancing security. Combining IR disruption with video steganography provides a layered defense against piracy and unauthorized access.

The system's success depends on the type of camera; some advanced cameras may bypass IR interference. IR lights affect only recordings near the screen, so distant or zoomed recordings might still be possible. Matlab-based steganography is not optimized for real-time or large-scale use. Password security is critical, and weak passwords risk unauthorized access. Alerts require stable network connections. The system also does not prevent piracy from post-theatre leaks.

Future work could include adaptive IR modulation to counter advanced cameras and expanded IR coverage with sensors to detect recording attempts. Improving steganography for real-time use and adding multi-factor authentication will strengthen security. AI monitoring can help detect suspicious activity. Blockchain could secure logs of authorizations and alerts. Additionally, watermarking techniques can help trace pirated content online beyond theatre protection.

Conclusion

The integration of infrared interference with cryptographic watermarking offers a promising solution to combat movie piracy in cinema halls. By disrupting unauthorized recording in real-time and embedding traceable information into video frames, this dual-layered system not only deters piracy attempts but also enables the identification of content leakage sources. The inclusion of LSM and GPS modules further enhances the responsiveness of the system by alerting authorities as soon as suspicious activity is detected. With a focus on automation, viewer safety, and ease of integration, the proposed method stands as a practical and scalable approach for the film industry to safeguard its intellectual property.

References

[1] B. Kalaimathi, S. Alamelu Alias Rajasree, M. Kowsalya, M. Gurusaren, S. Dinesh Kumar, and R. Balasubramanian, "Enhancing Movie Piracy Prevention through Automated IR Transmission and Steganographic Method," *Proceedings of the 5th International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 2024.

[2] Y. Fouzar, A. Lakhssassi and M. Ramakrishna, "A Novel Hybrid Multikey Cryptography Technique for Video Communication," in *IEEE Access*, vol. 11, pp. 15693-15700, 2023

[3] P. S. K. Narayanaswamy, R. Ahmed, P. R. K., and A. R. J., "Proposing Forensic Watermarking Techniques for Detecting Movie Piracy Through Camcorders," *Proceedings of the International Conference on Electronics, Computing, Communication and Control Technology (ICECCC)*, Bengaluru, India, 2024.

[4] H. Mareen, et al., "Camcording-Resistant Forensic Watermarking Fallback System Using Secondary Watermark Signal," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 9, pp. 3403–3416, Sept. 2021.

[5] T. P. Rani, S. Susila Sakthy, K. S. Saravanabharathi, and R. Yeshwanth, "Piracy Estimation and Detection in Movies and OTT Series using Similarity Functions and Deep Learning Techniques," *Proceedings of the International Conference on Emerging Research in Computational Science (ICERCS)*, Coimbatore, India, 2024.

[6] Nanditha L, Sanjana M G, Srinidhi R, Virinchi S Rao, Tejaswini C S, "A novel approach to Develop a Movie Piracy prevention system", International Journal of Advanced Research in Science, Communication, and Technology, Vol. 2-Issue 2, June 2022.

[7] Chethanya. K, Chirag. P, Lohith. G, Naveen. V, "Design and Implementation of an Automated Anti-Piracy System", IJARIIE, Vol. 7-Issue 4, 2021.

[8] A.M. Prasanna Kumar, Bharathi Gururaj, "Deterrence of piracy employing IR Transmitter and Steganography system", ACS Journal for Science and Engineering, Vol. 1- No. 2- September 2021

[9] Dr.Sheeja Augstin, Aleena Nair, Aravind Ajit, Aravind R, Jayanth Indalvai Reddy, "Tracking of Video Piracy using unique Identifier", International Journal of Engineering Applied Sciences and Technology, Vol. 8-Issue 7, December 2021.

[10] BVV Rajesh Kumar et.al, "Reduction of Movie Piracy using an Automated Anti-piracy Screen Recording System", International Conference on Information, Vol. 1 - No. 2, September 2021.

[11] Chandana P S, Akshatha H M, Rekha D M, Raghavendra Y M, "Movie piracy reduction using automated infrared transmitter screen system and steganography technique", International Journal of Engineering Research and Technology (IJERT), Vol. 8- Issue 13. 2020.

[12] Dr. Venkata Kishore Kumar Rejeti, J.Gowtham, B. Hemanth, " Preventing Movie Piracy", International Journal of Advanced Research in Science, Engineering, and Technology, Vol. 7– Issue 1, January 2020.

[13] B.P. Arjun, N. Harshavardhana Reddy, H.S.Bharath, B.Poornima, "Movie piracy tracking system using video steganography", International Journal of Research in Engineering, Science, and Management, Vol. 3 – Issue 2, February 2020.

[14] Sanju D J, Shwetha S, Spandana S, Tejaswini B V, Yogalakshmi H R," Movie Piracy Prevention using Automated Infrared Transmitter screen" , International Journal for Scientific Research and Development, Vol. 8-Issue 4, 2020.

[15] Divya Rani, Harish Kumar R, Harsha S N, Manjunath C W, Vanishree M L, " Movie piracy tracking system", Journal of Emerging Technologies and Innovative Research, Vol. 7-Issue 6, June 2020.

Copyright & License:

© Authors retain the copyright of this article. This work is published under the Creative Commons Attribution 4.0 International License (CC BY 4.0), permitting unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.