IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12210

Tackling Movie Piracy enigma employing Automated Infrared Transmitter Screen System and Steganoanalysis Techniques

Achyutha Prasad N[1], Vismaya K R[2], Tejashwini V[3], Samhitha B[4], Sathwik C M[5]

Professor and Head of Computer Science and Engineering, East West Institute of Technology Bengaluru, India[1]

Research Intellect Computer Science and Engineering, East West Institute of Technology Bengaluru, India[2-5]

Abstract: The major objective of our project is to lessen movie piracy. The most common method of film piracy is to recorda movie being seen in a theatre with a camera, edit the footage, and produce a better image. In order to reduce and stop moviepiracy, the goal of our initiative is to stop people from recording videos of films that are being viewed in theatres. Even if we are unable to completely eradicate it, we can lessen the costs brought on by piracy. We employ infrared radiations for this purpose since IR rays have the ability to be recognized by cameras but not by human eyes. Therefore, we employ this characteristic of infrared to stop the camera from recording the film. Given that direct infrared is harmful to humans, In the upper and lower portions of the bandwidth, we use the near-infrared spectrum.

Keywords: Infrared light; RFID; GSM; GPS;

I. INTRODUCTION

In order to give copyrighted content "appropriate" protection in the internet digital world, India recently added some digital rights management (DRM) requirements to the Indian copyright legislation. The movie business has constantly sought to portray online piracy as a severe danger, and it was one of the main groups that lobbied for the new DRM regulations in India. The Indian film industry also makes heavy use of John Doe orders issued by the country's high courts to bar Internet users from visiting websites thought to be offering pirated content. In light of the new DRM regulations in India, this study examines two issues:

(1) Is the Indian film business at risk from online piracy?
(2) Are the current steps being taken by the film industry the best ones to combat online piracy?

This report challenges industry assertions that online piracy is pervasive in India using data from a comprehensive empirical survey conducted in India. The findings of the empirical survey are also supported by data on Internet usage in India. So, in the proposed project, we intend to create an anti-piracy system for the film industry by using a modulo operator-based steganography technique in PYTHON and designing an IR-based screen to disable mobile recording and alert system.

Fig 1.1 Movie Piracy

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12210

The global film industry brings in trillions of dollars each month. We could also lessen the losses brought on by piracy for thefirst 15 to 30 days by implementing our method. We could charge a premium for our solutions because they increase profits for the industry as a whole (every country).

The movies are captured in one country and processed in another using an unidentified server before being released as a pirated version.Furthermore, recent digitization of movie prints using "Qube Cinema" technology has aided in obtaining clear pirated versionprints. This all occurs within the first 15-30 days of a film's release, after which a clear copy will be available.

Camera detecting systems are commonly used to prevent people from taking photographs or videos in restricted, prohibited, or secured areas. Cameras are detected and usually confiscated.

II. LITERATURE REVIEW

A. Title: Watermarking to Track Motion Picture Theft

A digital watermark is a type of maker that is embedded in a noisy signal such as audio, video, or image data. The music industry believes that unauthorised P2P trading of music flies has reduced revenue. The film industry fears that the same thing will happen to movies. However, the piracy issues in these two domains are not the same.

In this paper, we take an interesting look at movie piracy and compare it to music piracy in terms of piracy source and potential revenue impact. We do not address issues of politics, business, ethics, sociology, or copyright law directly, but instead identify relatively uncontroversial areas where technology, specifically digital watermarking, can make a significant contribution.Advantages: Steganography seeks imperceptibility to human senses. Disadvantages: The PSNR ratioperformance is poor and ineffective for standard datasets.

B. Title: The Fact and Fiction of camcorder piracy

Michael Geist, an Internet law professor, examines the arguments surrounding movie camcorder piracy and believes that factsshould be distinguished from fiction. A steady stream of reports has asserted in recent months that movie piracy is on the rise in countries around the world, resulting in hundreds of millions of pounds in lost revenue. In response to the prevalence of illegal camcording - the practise of videotaping a movie directly from the screen in a theatre and transferring the copy onto DVDs for commercial sale - the major Hollywood studios have launched incentive programmes for theatre employees to report camcording incidents and threatened to delay the release of their top films.

While the reports have garnered significant attention, a closer examination of the industry's own data reveals that the claims are primarily based on fiction rather than fact.

III. EXISTING SYSTEM

Electronic device jammers, for example, disrupt the operation and functionality of the device itself. This effectively prevents the camera from capturing videos and photos. However, in places where other devices such as cell phones, laptops, and so onare required, this system fails to provide a suitable environment. In recent years, even infrared rays have been used to preventvideo recording.

Apple Inc. was granted a patent for developing a system that would prevent concertgoers from taking bootleg footage. This system employs infrared projectors in four corners of the room to emit IR rays, preventing the capture of photos and videos.

IV. PROPOSED SYSTEM

The main goal is to create an anti-piracy system for the film industry using a modulo operator-based steganography techniquein Python, as well as to design an IR-based screen to disable mobile recording and alert system.

In our project, we use the property of light that is not visible to naked eyes but can be picked up by cameras; only visible lightcan be detected by human eyes. However, light rays such as IR and UV cannot be seen with our eyes, but cameras can easily capture images of them. So, when we project picture shows in theatres, we send original visible rays that assist us in seeing movies in theatres, along with a mix of other invisible light beams.
The innovation in our project is in the design, where we use an inbuilt IR burst transmitter that sends high intensity

DOI: 10.17148/IJARCCE.2023.12210

infrared rays along with the movie projection. This entire infrared blaster and projector system works in tandem. In contrast to the previous case, where the IR system may or may not be operational. As we focus on preventing piracy in the film industry, itis critical that the system works in tandem with the movie being played. As a result, integrating the IR system with the projector aids us in achieving this goal.

This issue can be mitigated by placing infrared LEDs along theatre screens. Because infrared light is invisible to the human eye, it causes no problems for the audience. However, when the same IR light falls on the camera, it creates glares and causes disruption in the recorded video using this method.

We can reduce camcorder piracy by lowering the quality of the recorded video. The innovation in our project is in the design,where we use an inbuilt IR burst transmitter that sends high intensity infrared rays along with the movie projection. Thisentire infrared blaster and projector system works in tandem. In contrast to the previous case, where the IR system may or may not be operational. As we focus on preventing piracy in the film industry, it is critical that the system works in tandem with the movie being played. As a result, integrating the IR system with the projector aids us in achieving this goal. The proposed model has three goals.

- ➢ Creating an Infrared Transmitter Screen to Avoid Mobile Recording
- ➢ Steganography is a technique used to conceal a secret key in order to prevent piracy.
- ➢ Using GPS, a GSM-based immediate alert is sent to the appropriate authorities to notify them of the location of the pirate.Maintaining the Specifications' Integrity

IR LED's- The infrared sensors are programmed to detect the presence or absence of partitions, causing lighting functions to change to accommodate the appropriate size space. These LEDs are embedded behind the screen and are controlled by a microcontroller. This technology works by capturing the pattern rather than the information when any capturing device flashes on IR light.

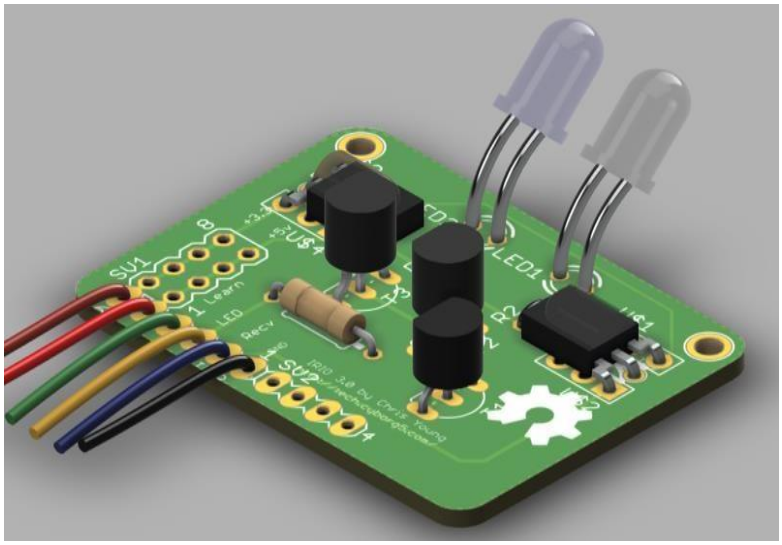

Fig 1.2 IR LED

GPS stands for Global Positioning System. By measuring the distance between satellites, it is possible to precisely identify locations on Earth. Cirocomm's MT 3318 GPS Receiver with high gain active patch antenna is used in this system. The GPS receiver communicated with the microcontroller via serial communication via UART1. The GPS receiver can track up to 51 satellites at the same time. The GPS receiver, as well as the 3.3V voltage regulator, transmit, receive, and power indication LEDs, are mounted on the PCB. The GPS receiver's output data is in NMEA (National Marine Electronics Association) format. It is a network of satellites that continuously transmit coded information.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12210

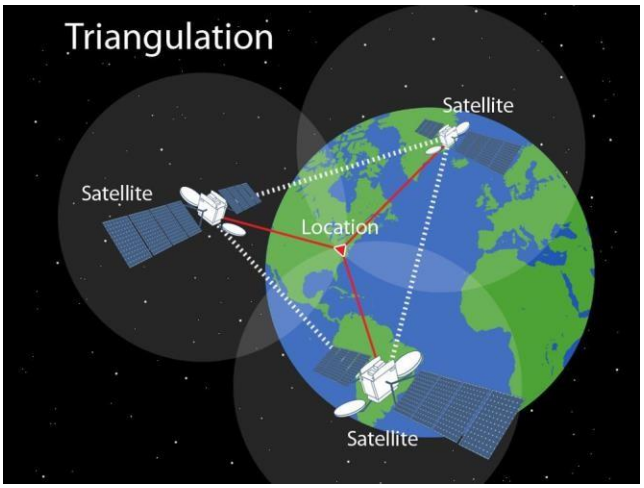

Fig 1.3 GPS (GLOBAL POSITIONING SYSTEM)

GSM Modem is an abbreviation for Global System for Mobile Communication. This GSM Modem accepts any GSM network operator SIM card and functions similarly to a mobile phone, complete with its own unique phone number. The advantage of using this modem is that you can communicate and develop embedded applications using its RS232 port. SMS control, data transfer, remote control, and logging are all simple to create. This GSM modem is a plug-and-play quad band GSM modem with high flexibility for direct and easy integration into RS232 applications. Voice, SMS, Data/Fax, GPRS, and an integrated TCP/IP stack are all supported. In text mode, this system employs a SIM 300 GSM module. The SIM300 GSM module provides 900/1800/1900MHz Tri-band for VOICE, SMS, DATA, and FAX in this system.. This module is controlled by the AT command. GSM Module recognise the AT command as an abbreviation for Attention command.

Fig 1.4 GSM card

Relay The relay is an electromagnetic switch that controls whether the IR is turned on or off.

LPC2148 is the ARM-7 module in our system. It serves as the system's primary controller unit. This unit receives input from various units such as an IR sensor and an engine switch, which it processes according to programming and outputs to the relay driver circuit and the GSM module. The ARM7 module requires 3.3V to operate.

1) Pre-processing: If the target string length is not a multiple of four, some less common special characters are concatenated at the end to make the string length a multiple of four. Each character of the target string was converted to ASCII and 7 bit binary for preprocessing. After that, every four bits are cut and converted to hexadecimal digits. Let the string be "Secret," with a length of 6. "" is appended to make it a multiple of four. As a result, the string becomes "Secret".

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12210

This target string's ASCII characters are 83, 101, 99, 114, and..., and their corresponding 7 bit binary is 1010011 1100101 1100011 1110010.....Concatenating it yields 10100111100101110001111110010... The hexadecimal digits are then A 7 9 7 1 F 2...

2) Embedding using modulo operator: By adjusting the amplitude values of the target samples, these hexadecimal digits are now embedded into the cover video. Cover video amplitudes are divided by 16. The remainders are then compared to the target hexadecimal digits, and the amplitudes of the cover video are adjusted so that the remainder matches the target hexadecimal digits

To avoid large changes, the amplitude boundary values 32760-32767 and 0-8 are treated differently. Assume the cover amplitude value is 32764 and we want to insert 1 as the target octal digit; if the proposed technique is used, the result is 32769, which is not within the range 0 to 32767 In this case, the backward differences are taken into account. That is, if the modified amplitude value is less than 0 or greater than 32767 when forward or backward differences are considered, the cover amplitude value is replaced by the other difference, i.e. backward and forward differences.

The secret string's 16-bit string length is stored in the first 16 samples using the standard LSB technique for extraction at the receiver side.

Extraction

At the receiver side, the string length is extracted from the first 16 amplitudes using the standard LSB extraction techniquebefore extracting the target data from stegovideo. Then the following steps must be taken:

1) Extraction using modulo operator: The affected (where the data is hidden) amplitude values are divided by 16 at the receiver side, and the remainders of this division are hidden hexadecimal digits. This is now sent to the post-processing technique in order to obtain the original target text.

2) Post-processing: The hexadecimal digits that result are now converted to their 4 bit binary equivalent. A binary string is formed by concatenating these four bits. Then, every 7 bits are removed and converted to their decimal equivalent. To obtain the original target string, the characters of these ASCII values are concatenated according to the string length.

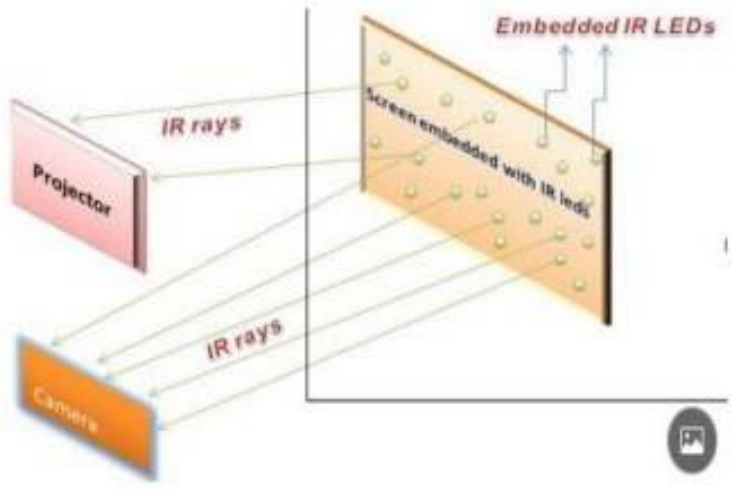

Fig 1.5 Overall implementation

Steganography is used to create a master copy of video frames in which permitted operator details, operator location, distributor names, and other information are hidden in video frames that are invisible to human eyes. A video player powered by Python will play video frames. While playing video in the theatre section, it will look for hidden keys in video frames and,if a key is found, it will allow you to play the video. At the same time, an alert will be sent to the microcontroller to turn on he IR transmitters, which will block the mobile recording mode by sending IR beams. If the key is denied, the user's GPSlocation will be sent to the appropriate authority via SMS for action..

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023

DOI: 10.17148/IJARCCE.2023.12210

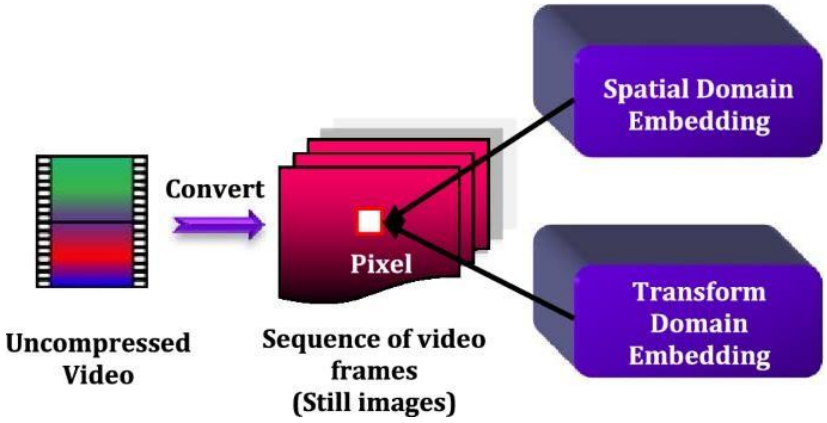

Fig 1.6 Working analysis

Video steganography

Because a video file is essentially a collection of images and sounds, most of the techniques presented for images and audio can also be applied to video files. As a result, video steganography is simply a combination of image and audio steganography. As a result, the combined evaluations, i.e., the evaluations for image and audio steganography, can be used to evaluate video steganography. The large amount of data that can be hidden inside video, as well as the fact that it is a moving stream of images and sounds, are two of its major advantages. A video stream is made up of frames, and the secret data is embedded as payload in these frames.

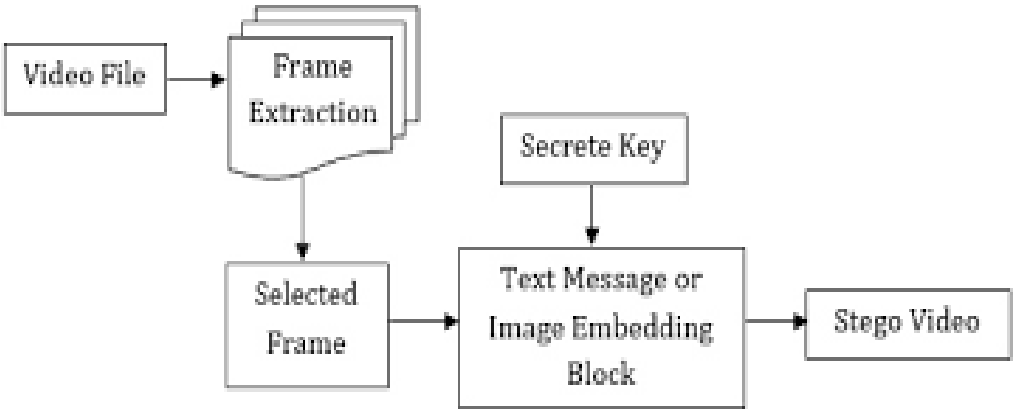

Fig 1.7 Block diagram of Video steganography

Applications and Advantages

- Confidential communication and secret data storage
- Data alteration protection
- Digital content distribution access control system
- Media database systems Steganography allows us to:

1. Possibility of concealing the existence of confidential data.
2. Difficulty of detecting hidden (i.e. embedded) data
3. Increasing the secrecy of encrypted data

- Modern Printers Leading manufacturers of digital and laser printers, including HP, use steganography.
- This system is intended to increase security.
- This system will be low in cost, power consumption, and accuracy.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 7.918 ⁜ Vol. 12, Issue 2, February 2023
DOI: 10.17148/IJARCCE.2023.12210

ACKNOWLEDGMENT

The sense of accomplishment and euphoria that comes with completing a task would be incomplete without mentioning the people who make it possible, whose constant guidance and encouragement propels our efforts to success. We would like to express our heartfelt gratitude to **Dr. Achyutha Prasad N**, Professor and (Head of the Department of Computer Science and Engineering, East West Institute of Technology), Bangalore, for his encouragement and guidance, as well as his timely inspection and guidance throughout the process. We also want to thank the members of the Computer Science and Engineering faculty, whose suggestions helped us overcome many seemingly insurmountable obstacles.

REFERENCES

[1] Y Chen, G Zhai, Z Gao, Ke Gu, W Zhang, M Hu, J Liu "Movie Piracy Tracking Using Temporal PsychovisualModulation", in IEEE conference 2019.
[2] J Bloom and C. Polyzois, "Watermarking to track motion picture theft," in Signals, Systems and Computers, 2004.Conference Record of the Thirty-Eighth Asilomar Conferenceon, vol. 1, Nov 2019, pp. 363–367 Vol.1.
[3] MEpstein and Stanton. "A method and device for preventing piracy of video material from theater screens", Oct. 4 2020,eP Patent App. EP19,990,923,789. [Online]. Available: https://www.google.com/patents/EP1040655a2?cl=en
[4] Karthik.S, Abhishek.P, Chandresh.P.M, Bharath. K.R, Mrs. Sahana Salagare "Anti-Piracy Screen using VLC" [Online].Available: http://www.ijettjournal.org.
[5] US Patent "Movie Film Security System Utilizing Infrared Patterns reference", [Online].Available:https://patents.google.com.
[6] Website "An Introduction to RFID Technology" reference [Online].Available: https://www.cs.colorado.edu.
[7] Website "A GSM Technology" reference [Online].Available: https://www.lifewire.com.C Hu, G. Zhai, Z. Gao, and X. Min, "Information security display system based on spatial psychovisual modulation," in2019 IEEE International Conference on Multimedia and Expo (ICME).