“VIDEO PIRACY DETECTION AND AVOIDANCE”

Submitted in partial fulfillment of the requirements for the degree of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE

Submitted by

P. ANEESHRAM BHAT
4NM20CS124
AKSHATA PRABHU
4NM20CS020

Under the guidance of
Dr. GEETHA V

DEPARTMENT OF INFORMATION TECHNOLOGY
NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA
SURATHKAL, MANGALORE - 575003
2022-2023

DECLARATION

We hereby declare that the project report entitled, **"Video Piracy Detection and Avoiding"** has been completed and written by us. To the best of our knowledge and belief, the work embodied in this report has not formed earlier the basis for the award of any Degree or similar title of this any other University or examining body. I give an undertaking that the material included in the report from other sources is duly acknowledged. I have incorporated all the changes as suggested by the Pre-submission presentation Committee, if any.

P. Aneeshram Bhat (4NM20CS124)
Akshata Prabhu (4NM20CS020)
N.M.A.M. Institute of Technology

Date: 30/09/2023
Place: NITK, Surathkal

CERTIFICATE

This is to certify that the project report entitled “VIDEO PIRACY DETECTION AND AVOIDING", submitted by P. Aneeshram Bhat (4NM20CS124) and Akshata Prabhu (4NM20CS020) is the bonafied work completed under my supervision and guidance in partial fulfillment for the award of Bachelor of Engineering (Computer Science) of N.M.A.M. Institute of Technology (NITTE). This report in any form has not been submitted to any other University or Institution.

Dr. Geetha V
Assistant Professor (Grade I)
NITK, Surathkal

ACKNOWLEDGEMENT

The portion of success is brewed by the efforts put in by many individuals. It is constant support provided by people who give you the initiative, who inspire you at each step of your endeavor that eventually helps you in your goal.This acknowledgement is a humble attempt to thank all those who were involved in this project work and were of immense help to me.

It is our privilege to acknowledge with deep sense of gratitude to our project guide Dr. Geetha V for her valuable suggestions and guidance throughout our course of study and project. Her excellent guidance made me to complete this task successfully.

We will be failing in duty if we do not acknowledge with grateful thanks to the authos to the references and other literatures referred in this project.

Last but not the least, we take pleasant privilege in expressing our heartful thanks to our friends who were of precious help in completing this project.

P. Aneeshram Bhat , Akshata Prabhu

Contents

List of Figures

1 Introduction

Internet piracy is the most popular trend in todays world. People prefer watching movies and series for free on pirated website rather than pay for Netflix or amazon prime due to which companies like Netflix has seen a drastic decrease in their number of users. Pirated video material gets over 230 billion views a year. 126.7 billion viewings worth of US produced TV episodes are pirated every year. Content creators spend a substantial amount of time creating their content. A lot of TV series you might see on Netflix take months to produce and a lot of money too. It is a bummer to put in all this effort and then your content gets downloaded for free. In some cases, users share their credentials with others and a single account is used for multiple access. Digital video piracy is costing the economy between $29.2 and $71 billion each year. The movie which is released today can be seen on pirated websites within 24hrs and people prefer watching the movie/series for free from pirated websites rather than paying for the movie and watching it in the theater. Illegal downloading of copyrighted materials takes up 24% of the global bandwidth. The country with maximum number of visits to pirated websites is United States with 17.380 billion visits per year, followed by Russia with 14.468 billion visits and India with 9.589 billion visits. Only China has recorder a relatively low total of 4.6 billion visits so far. Recent online piracy statistics show that over 50% of these recorded visits went to streaming sites, which remain the go-to tool for most users. However, torrent and direct-download portals are also popular. Annual global revenue losses from digital piracy are between $40 and $97.1 billion in the movie industry. By far the most common unauthorized access to content comes through illegal streaming, accounting for up to 80% of global online piracy. Beyond voluntarily sharing passwords, accounts can also be hacked and login credentials sold on black-market sites. Sensitive company content is constantly under threat from hackers. This could include internal video meetings, private virtual events, or a variety of confidential internal content. As mentioned above, even content that is meant for public consumption can be pirated and show up on unsavory sites, which can create lasting brand damage for the companies. From local creators to international producers, pirates threaten their livelihoods by using software to illegally download content or screen recorders to capture content and resell or distribute it.

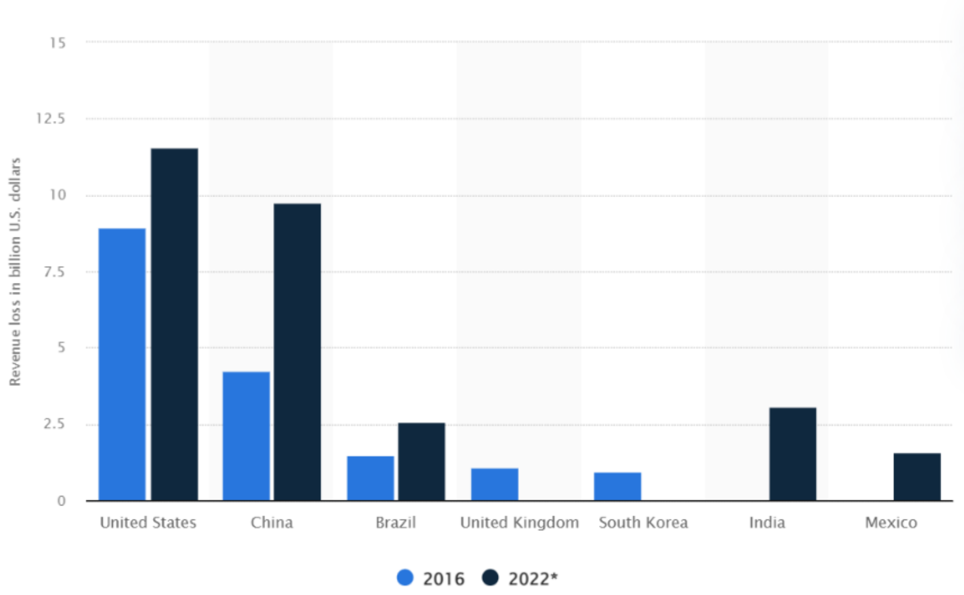

Figure 1: Online TV and movie revenue loss due to piracy in 2016 and 2022

Impact of video piracy on business

- Global Revenue Loss: According to a report by the Digital Citizens Alliance, global revenue losses due to online piracy were estimated to be around $29.2 billion in 2020. This includes losses across various industries, such as film, TV, music, software, and publishing.

- Film and TV Industry Impact: The film and TV industry has been particularly affected by video piracy. In a study conducted by the Motion Picture Association (MPA), it was estimated that the global film industry lost around $6.8 billion to piracy in 2019.

- Regional Variations: The impact of video piracy can vary significantly across different regions. Some countries or regions with weak copyright enforcement measures may experience higher piracy rates and subsequently greater losses for businesses.

- Streaming Services and Subscription Losses: With the rise of streaming services, video piracy has expanded to include unauthorized access to subscription-based platforms. A study by Parks Associates estimated that the revenue loss from credential sharing and piracy for OTT (over-the-top) video services would reach $12.5 billion by 2024.

2 Literature Survey

2.1 Watermarking

Video piracy remains a significant challenge in today's digital world. It involves the unauthorized distribution, reproduction, and sharing of copyrighted video content without proper licenses or permissions from the content owners. The advent of the internet and the proliferation of digital technologies have made it easier for individuals to copy, distribute, and consume pirated video content. Numerous websites and online platforms host pirated video content, allowing users to stream or download movies, TV shows, sports events, and other videos without proper authorization. These platforms often generate revenue through ads or subscription fees, despite the fact that they are distributing copyrighted material without permission. Many techniques have been invented to avoid video piracy, including digital rights management (DRM) systems, watermarking, content fingerprinting, encryption, geo-blocking, and legal actions against piracy websites. These measures aim to safeguard the rights of content creators and distributors while encouraging consumers to access and enjoy content through legitimate channels. Watermarking is a technique used to embed information or a pattern within digital media, such as images, videos, audio, or documents. The purpose of watermarking is to identify the creator or owner of the media, protect intellectual property, and track the distribution of content. Watermarks are typically added without significantly affecting the overall quality or usability of the media. By embedding visible or invisible identifiers within digital media such as images, videos, and documents, watermarking serves as a digital signature that establishes ownership and origin. These digital markers are meticulously designed to withstand common alterations like compression, cropping, and resizing, ensuring their detection even after modifications. Watermarking is pivotal in discouraging unauthorized use and distribution of media, as it introduces an enduring link between the content and its rightful creator. While not impervious to determined infringes, watermarking forms a pivotal component of the broader endeavor to protect digital assets and maintain the integrity of intellectual property in our increasingly digitized world. But the disadvantage with watermarking is that the watermark can be easily removed hence other video piracy avoiding technique is implemented along with watermarking to increase the safety. Watermark can be either embedded to a single frame or multiple frames based on the content creators wish.

Author	Methodology	Observation
J.V. Bagade et al. [1]	A robust Discrete Wavelet Transform (DWT)-based blind digital video watermarking scheme with scrambled watermarks based on scene changes for authentication of digital video.	It is robust against different image processing attacks like addition of noise, median filtering and cropping. It embeds different parts of a single watermark into different scenes of a video and restricts partial removal of the watermark.
Hao Ding et al. [2]	The proposed method specifically targets resisting recompression attacks when the quantization parameter undergoes significant increase. Ensures robust video watermarking with low complexity.	The method utilizes texture and motion information of the video to identify invariances in video content under different quantization parameters, improving its resistance. The method also effectively limits the degradation in video perceptual quality.
Abhinav Gupta et al. [3]	Watermarking of MPEG-4 Videos by modifying Discrete Cosine Transformation (DCT) coefficients	The technique is not only robust to synchronization errors but also improves the quality of videos using local adaptive gain technique. The disadvantages of this approach is noise addition due to recompression.
Zehui Ke et al. [4]	Robust Video watermarking based on deep neural network and curriculum learning	This paper proposes a video watermarking method for watermarking of sliced videos. Lee et al. uses a simple CNN for embedding and extraction without any resolution dependent layers.
Shaohui Liu et al. [5]	An Improved Spatial Spread-Spectrum Video Watermarking guided by JND(Just Noticeable Distortion) model IN DCT domain	Spatial video watermarking algorithm can ensure the robust better than many other kinds of watermarking algorithms in compressed domain.

Manoj Pandey et al. [6]	A comparative study of various digital image watermarking techniques: Specific to hybrid watermarking	The primary goal is to find techniques that balance imperceptibility (how well the watermark is hidden in the content) and robustness (how well the watermark survives various attacks).
Kh. Manglem Singh et al. [7]	Uses visual cryptography, scene change detection, preprocessing of the watermark. The frames are marked using LSB substitution to generate random number for embedding based on a given seed or key.	Withstand different types of video attacks, especially frame averaging, frame dropping, frame swapping and interpolation, besides different types of malicious attacks such as JPEG compression, sharpening, lightening, etc.
Jing Sun et al. [8]	Anti-compression watermarking algorithm based on moving object detection,that includes: moving object detection and watermark embedding.	A highly efficient method that is robust against recompression and has little impact on the video visual quality.
Ta Minh Thanh et al. [9]	Embedding the visible watermarking through the adaptive cross-correlation (ACC) method.	The method serves two purposes:1) asserting ownership of the video and 2) identifying authorized users. Experimental results demonstrate the suitability of the proposed method for digital e-commerce and its robustness against minor attacks.
Xin Zhong et al. [10]	A Robust Image Watermarking System Based on Deep Neural Networks.	This paper introduces an automated image watermarking system. The proposed blind image watermarking system achieves its robustness property without requiring prior knowledge of possible distortions on the marked-image.

2.2 Prevention Techniques

Preventing video piracy is very important these days to protect the revenue of content creators and distributors. Many prevention techniques has been introduced to reduce the possibilities of video piracy. For example Netflix avoids password sharing, screen sharing, screen recording etc. Preventing video piracy is essential for protecting the intellectual property rights of content creators and sustaining the financial integrity of the film and entertainment industry. To achieve this, a comprehensive set of strategies can be employed. These include implementing Digital Rights Management (DRM) to secure content from unauthorized access, using watermarking to trace the source of pirated material, and employing encryption to safeguard video files. Secure streaming services and legal enforcement also play pivotal roles, as do public awareness campaigns, user authentication, and global release strategies, all of which collectively dissuade piracy by providing accessible, high-quality, and affordable legal alternatives. This multifaceted approach combines technical, legal, and educational measures, ensuring the protection of intellectual property and the long-term viability of the entertainment sector.Additionally, fostering international cooperation and agreements for combating piracy across borders, addressing the proliferation of torrent and streaming sites, and continuously evolving security technologies are integral aspects of this multifaceted approach, ensuring the protection of intellectual property and the long-term viability of the entertainment sector.

Technique	Observation	Drawback
Visible Watermark	Adding a visible watermark involves overlaying a distinctive mark onto video content to indicate ownership, prevent unauthorized use, and deter piracy. Placing a transparent logo or symbol of the content creator or distributor on a corner of the video is a straightforward way to add a visible watermark.	Visible water can disrupt the viewing experience as they can obsure important parts of the video. Determined pirates can attempt to remove or edit the watermarks, especially if they are not heavily integrated into the videos visual elements. Watermarks can clutter the content, especially if they are too large or intrusive, making it difficult for viewers to fully appreciate the content.
Invisible watermark	Invisible watermark is added to digital content mainly using frequency domain techniques which modifies the least significant bits (LSBs) of the frequency coefficients in the Discrete Cosine Transform (DCT) domain or using Spread spectrum technique in which the watermark data is spread across the frequency spectrum of the content using a pseudo-random sequence.	This method overcomes the disadvantage of quality degradation as observed in visible watermark but if pirates identify the method used to embed invisible watermark then they can rewrite the code to remove the watermark or change the watermark which can distort the video quality. Invisible watermarks can carry only a limited amount of information due to the constraints of embedding imperceptible changes. This limits their usability for encoding complex metadata.

Digital Rights Management (DRM)	DRM technologies encrypt videos and restrict their playback to authorized devices and platforms. This prevents users from easily copying or redistributing the content. Popular DRM solutions include Microsoft PlayReady, Google Widevine, and Apple FairPlay.	DRM can introduce complexities for legitimate users. DRM-protected content might not be compatible with all devices and platforms. DRM systems often collect user data for authentication and tracking purposes, which can raise privacy concerns about the amount and nature of data being collected.
Geoblocking and IP Restrictions	Geoblocking and IP restrictions are methods used to control the distribution of digital content by limiting access based on the geographic location or IP address of the user. Restrict access to your video content based on geographic location or IP addresses. This helps in controlling the distribution of content to specific regions.	Geoblocking can inadvertently exclude legitimate users who are traveling, living in different regions, or using VPNs for security reasons. Determined pirates can easily bypass geoblocking by using VPNs or proxy servers to mask their true IP addresses, allowing them to appear as if they are accessing the content from an authorized region. Implementing and maintaining geoblocking and IP restrictions require ongoing management and updates.
Encryption and decryption	Encryption and decryption are widely used methods to protect digital content, including videos, from unauthorized access and piracy. Encrypting video files during storage and transmission can prevent unauthorized access. This makes it difficult for pirates to intercept or copy the content without proper decryption keys.	Encryption requires users to have the necessary decryption keys or software to access the content. This can introduce complexities for end users, especially those who are not tech-savvy. Managing encryption keys securely can be challenging. If keys are lost or compromised, users might lose access to their own content. Encrypted content might not be compatible with all devices.

2.3 Outcome of Literature Survey

- Visible watermark is a type of watermark used mainly to avoid video piracy. They are placed in a way that does not obscure the main content but is still easily noticeable and difficult to remove or alter without leaving traces. They can be semi transparent to allow viewers to see the underlying content, but they are designed to be prominent enough to serve as a clear indicator of ownership or copyright protection.

- An invisible watermark is a technique used to embed information or metadata into digital content, such as images, videos, audio, or documents, without altering the perceptible quality of the content. The watermark is called "invisible" because it is not readily visible to the naked eye, but it can be detected and extracted using specialized software or algorithms. The invisible watermarking techniques are mainly used for copyrights protection, ownership identification, detection of illegal source redistribution, etc. The invisible watermarking provides more security to video with less distortion, though the visible watermarks protect the digital data in more active manner

- According to the domain of watermark embedding, traditional video watermarking methods can roughly divide into three schemes: spatial domain, transform domain, and compressed domain. In addition, with the development of deep learning, many image watermarking methods based on deep learning have emerged in recent years, mostly based on CNN-based auto-encoder and generative adversarial networks. Spatial video watermarking algorithm can ensure the robust better than many other kinds of watermarking algorithms in compressed domain. The watermark can be encoded for different purposes, such as increasing the perceivable randomness for additional security via encryption methods or restoring the impact of noise via error correction codes for watermark integrity under attacks.

2.4 Problem Statement and Objective

Design and development of video/movie piracy detection and avoidance using watermarking and machine learning and deep learning algorithm. The main goal of this project is to reduce the possibility of video piracy by implementing robust watermarking techniques that deter unauthorized distribution and enable efficient tracking and enforcement against copyright infringement.

Objectives:

- To design and develop invisble/visible watermark based video/movie piracy detection to detect the occurrence of video piracy.
- To design and develop video/movie piracy avoidance through Video Recording detection by avoiding camrecording and screenshots.

3 Watermarking

In today's world where video piracy is a huge threat in business, many techniques has been introduced to avoid video and movie piracy. The most popular and widely used technique is watermarking. It is used to deter video piracy and protect copyrighted content. Watermarks are unique identifiers or logos that are superimposed onto the video frames. They serve as a visible or invisible mark, helping to identify the source of the video and discourage unauthorized distribution. Visible Watermark is visible on the surface of the image or video and is often used to indicate ownership or copyright. It can be a logo, text, or an image overlaid on the original content. Visible watermarks are easily noticeable and serve as a deterrent against unauthorized use. Invisible Watermark also known as digital watermarking, this type of watermark is not visible to the human eye and is embedded within the data of the image or file. Invisible watermarks are used for tracking and authentication purposes without affecting the visual appearance of the content. There are different techniques of adding watermark, such as frame-by-frame watermarking, where a watermark is embedded into each individual frame of the video, or single-frame watermarking, where the watermark is added to only one frame of the video, such as the beginning or end, to provide copyright information or ownership details. The choice of technique depends on the level of protection needed and the trade-off between watermark visibility and the potential impact on the viewer's experience.

3.1 Visible Watermark

A visible watermark is a distinct and intentionally noticeable identifier or graphic element that is added to digital content, such as images, videos, or documents. It serves various purposes, including branding, copyright protection, ownership attribution, and discouraging unauthorized use or distribution of the content. Visible watermarks are placed on top of the original content, making them immediately visible to viewers. They are a means of indicating ownership and asserting intellectual property rights. They can take the form of text, logos, symbols, patterns, or other graphical elements that are overlaid onto the content. Companies and individuals often use visible watermarks to brand their content, establishing a clear connection between the content and its source. Visible watermarks can deter copyright infringement by providing a clear indication of ownership and copyright information. The position and opacity of the watermark are carefully chosen to balance visibility with content aesthetics. Watermarks are often semi-transparent to avoid obstructing the underlying content.

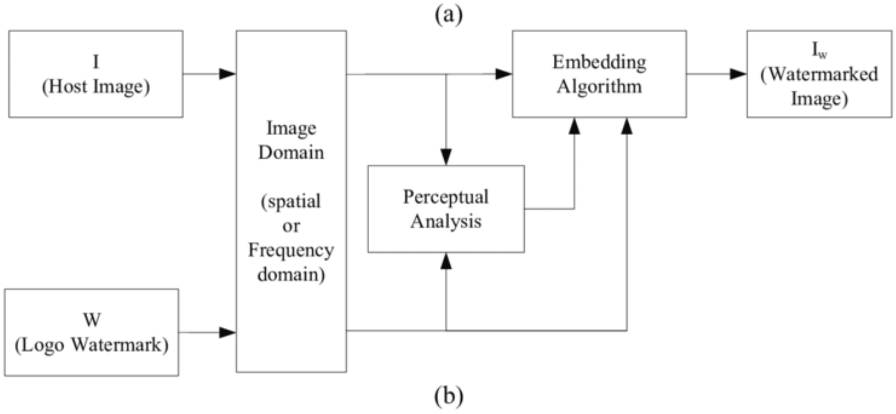

Figure 2: Visible Watermarking

While visible watermarks deter casual misuse, they may impact the viewer's experience and the content's aesthetics. Determined infringers might still attempt to remove or cover visible watermarks.Visible watermarks are typically placed on lower-resolution or preview versions of content. High-quality versions are often needed for legitimate uses, and protecting them can be challenging with visible watermarks alone.

3.2 Invisible Watermark

Invisible watermark is a discreet and imperceptible form of embedded data within digital content, such as images, videos, audio, or documents. They are designed to be hidden within the content while still carrying valuable information for various purposes. Invisible watermarks are crafted to be indistinguishable from the original content, ensuring that they don't affect the visual or auditory quality. These watermarks often encode data such as ownership information, copyright details, or unique identifiers that are difficult to detect without specialized tools. Invisible watermarks can be embedded in spatial or frequency domains, using techniques such as spread spectrum, quantization, or frequency modulation. Robust invisible watermarks are resistant to common alterations, such as compression, cropping, or image manipulations. Some methods use cryptographic techniques for added security. Specialized software or algorithms are required to detect and extract invisible watermarks from content.

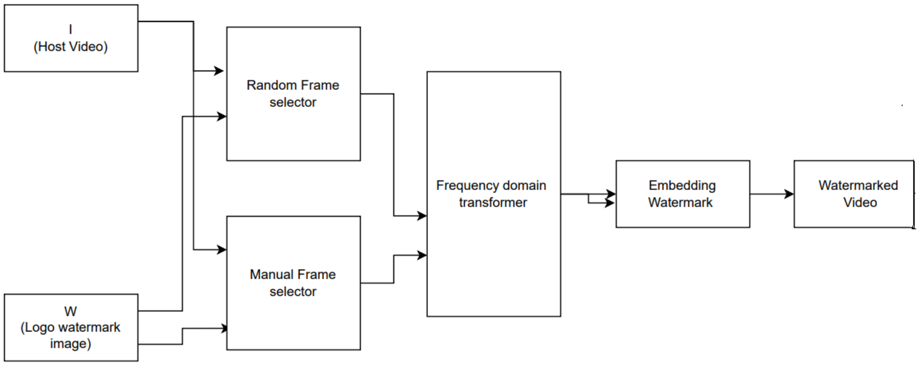

Figure 3: Invisible Watermarking

While invisible watermarks offer greater stealth compared to visible watermarks, determined individuals with advanced tools and skills might still attempt to remove or alter them.

In summary, invisible watermarks serve as a covert method for protecting digital content from unauthorized use and distribution. By encoding essential information within the content itself, they provide a way for creators to maintain control over their intellectual property while minimizing the impact on the user's experience. Invisible watermarks are a valuable tool in the realm of copyright protection and content authentication.

3.3 Implementation

"In our implementation, we employed a Python script that leverages the OpenCV library to seamlessly embed invisible watermarks into video content, strengthening its protection against unauthorized distribution and piracy. The implementation can be summarized as follows:

1. Video Input: We began by specifying the path to the target video (‘input-video-path‘) that we aimed to watermark. The script utilizes the cv2.VideoCapture function to open and read the video, extracting essential properties such as frame rate and dimensions.

2. Watermark Image: We selected a watermark image (‘watermark-image-path‘) that we intended to embed into the video. This image serves as the unique identifier, and we employed it with the ‘cv2.imread‘ function, using the ‘cv2.IMREAD-UNCHANGED‘ flag to preserve transparency.

3. Output Video: To create the watermarked video, we defined an output path (‘output-video-path‘) and set up a VideoWriter object with the XVID codec. The frame rate and dimensions of the output video were set to match those of the input video.

4. Frame Processing: We initiated a loop to iterate through each frame of the input video. For each frame, we performed the following actions:

   - Resize Watermark: We resized the watermark image to match the dimensions of the video frame, ensuring a seamless fit.

   - Alpha Blending: We applied alpha blending to merge the video frame with the resized watermark image. The alpha value (‘alpha‘) controlled the blending intensity, making the watermark perceptually invisible but reliably embedded.

- Write and Display: The merged frame was written to the output video using ‘out.write‘, and for visual inspection, it was displayed using ‘cv2.imshow‘. The latter step allowed us to verify the watermark’s imperceptibility but may be omitted in production.

- User Interaction: We included a feature that allowed the script to be terminated prematurely by pressing ’q’.

5. Cleanup: After processing all frames, we released the resources associated with the input and output videos using ‘cap.release()‘ and ‘out.release()‘. Additionally, any open OpenCV windows were closed with ‘cv2.destroyAllWindows()‘.

   By implementing this approach, we successfully embedded invisible watermarks into the video, enhancing its security without compromising the viewing experience. This technique can be a valuable asset in the fight against video piracy and unauthorized redistribution, as it facilitates content tracking and ownership verification."

4 Video Recording Detection for Mitigating Video/Movie Piracy

The protection of copyrighted videos and films against rampant piracy has become an urgent problem in an era where consumption of digital content is the norm. In-depth analysis of the 'Video Recording Detection for Mitigating Video/Movie Piracy' concept is provided in this paper. This new strategy is aimed at protecting intellectual property and preventing unauthorised replication and distribution. The risk of piracy is rising along with the popularity of internet streaming, endangering the work of content producers. The integration of a technology, notably the YOLO (You Only Look Once) object detection model, is explored in this paper in order to create specific software that can detect and prevent unauthorised video recording while it is being played back. This software may be smoothly incorporated into devices like laptops to create a strong line of defence that can identify and stop possible pirate efforts. This study explores the mutually beneficial relationship between innovative technological advancements and content protection, emphasising how video recording detection can both protect the integrity of digital media and improve the groundwork for intellectual property rights in the digital age.

4.1 YOLO Object Detection Model

1. Load pre-trained Model: In this step, the process begins by loading a pre-trained YOLO model. The model consists of pre-learned weights and architecture from a deep learning framework like TensorFlow or PyTorch. These weights encode knowledge gained from extensive training on large datasets and will be used to make predictions about objects in images or video streams.

2. Load Input Image/Video Stream: This step involves loading the input data, which can be an image or a stream of video frames. The input data serves as the target for object detection. The model will analyze this data to identify and locate objects within it.

3. Divide Image into Grid: The input image is divided into a grid of cells, each responsible for detecting objects within its boundaries. This grid structure helps to efficiently scan the entire image and identify potential object locations.

4. Generate Anchor Boxes: Anchor boxes are predefined boxes of different sizes and aspect ratios. These boxes serve as references for predicting bounding box dimensions during object detection. By comparing detected features to anchor boxes, the model can estimate the size and shape of objects.
5. Extract Features: Feature maps are extracted from the input image using convolutional layers. These feature maps capture important visual patterns and details in the image. The model uses these features to make predictions about the presence and characteristics of objects.
6. Predict Objects and Class Probabilities: For each grid cell, the model predicts two main things: the objectness score (the likelihood of an object being present) and class probabilities for different object categories. This step assigns a confidence score to each object detection and predicts the likelihood of it belonging to different classes.
7. Calculate Box Adjustments: The model calculates adjustments for the predicted bounding box coordinates based on the anchor boxes and the grid cell positions. These adjustments refine the initial estimates of object positions and sizes.
8. Non-maximum Suppression(NMS): Non-maximum suppression is applied to the predicted bounding boxes to remove duplicate and low-confidence detections. This step ensures that only the most accurate and relevant detections are retained, eliminating redundancy.
9. Draw Bounding Boxes: Once the most accurate detections have been identified through NMS, bounding boxes are drawn on the original image to highlight the location and extent of detected objects. This visualization provides a clear representation of the model's predictions.
10. Display or Output Results: The annotated image with the drawn bounding boxes is displayed to the user or saved to an output file. This step allows users to visually inspect the object detection results or use the annotated data for further analysis.
11. End: Indicates the completion of the object detection process.

This flowchart outlines the essential steps involved in the YOLO object detection model, enabling the identification and localization of objects within images or video streams. It showcases the complexity of the model's operations and highlights how it transforms raw data into meaningful visual information.

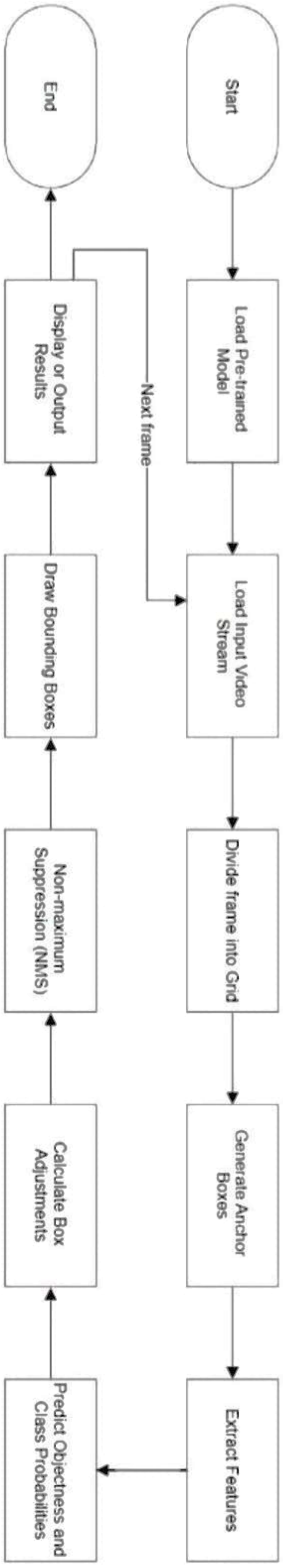

Figure 4: Flowchart-YOLO object detection model

4.2 Implementation

1. Camera Input:This is the starting point of the process. The system receives a continuous input video stream from a camera.
2. YOLO Object Detection: The input video stream is processed using the YOLO object detection algorithm. YOLO divides the video frames into a grid and predicts bounding boxes and class probabilities for detected objects.
3. Object Classified(Decision): This step checks whether the YOLO algorithm has successfully classified any object in the video frame as a phone.
4. TRUE - Display Warning Label: If the YOLO algorithm successfully detects a phone in the video frame, a warning label is displayed. This warning could inform users about potential privacy concerns or prohibited activities.
5. Pause Video: The system pauses the video playback to bring attention to the detected object and the warning label.
6. FALSE - Rescan to Reclassify the Object: If the YOLO algorithm does not detect a phone in the video frame or if there's uncertainty, the system can trigger a reclassification process. This could involve reprocessing the current frame or waiting for the next frame to arrive.
7. Show Pop-up Window with the Detected Object in Frame: If the YOLO algorithm detects an object (not necessarily a phone) in the video frame, the system can display a pop-up window showing the object that has been detected. This can help users understand what triggered the warning label or allow them to verify the object themselves.

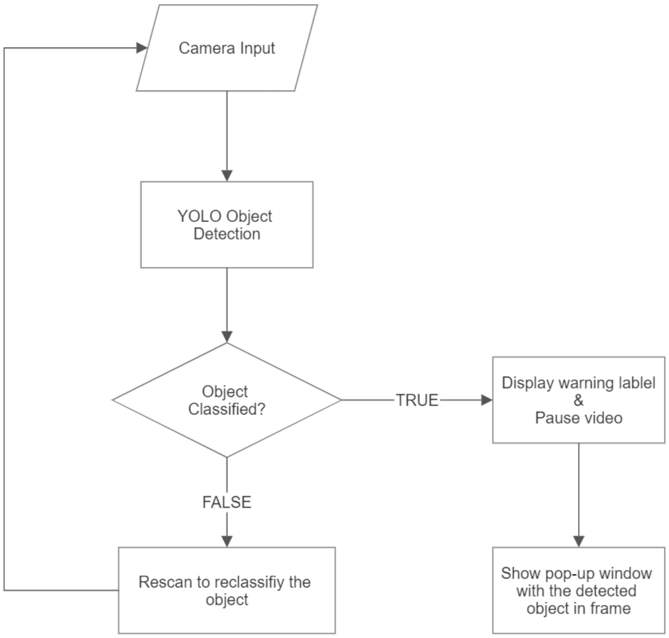
Camera Input
YOLO Object Detection
Object Classified?
TRUE
Display warning lablel & Pause video
FALSE
Rescan to reclassifiy the object
Show pop-up window with the detected object in frame

Figure 5: Design implementation

5 Results and Discussions

Input	Method	Output	Observation
Video taken from far using a phone	Color Distribution	98.41%	In this method we observe that 98.41% of frames have difference in the pixel shade. Here the comparison is made in each and every frame and then the overall difference in number of frame is calculated.
Video taken from near using a phone	Color Distribution	82.57%	In this method we observe that 82.57% of frames have difference in the pixel shade. Here the comparision is made in each and every frame and then the overall difference in number of frame is calculated.

Video taken from near using a camera	Color Distribution	20%	In this method we observe that 20% of frames have difference in the pixel shade. Here the comparison is made in each and every frame and then the overall difference in number of frame is calculated.
Original video trimmer	Duration	Video1: 8.23 Video2: 5.33	In this method we are calculating the time duration of both the videos and comparing if its same. If it isn't then we can conclude that the 2nd video is not the original video
Original video cropped	Height and width comparison	Resolution of Video 1: 1920x1080 Resolution of Video 2: 1280x720	In this method we calculate the height and width of both the videos and compare if its same. If it isn't then we can conclude that the 2nd video was formed by cropping the original video.
Video with audio	Audio comparison	Overall audio difference between videos: 0.13	In this method we calculate the difference in the audio. If there is a difference the we can conclude that the 2nd video is not the original video.

6 Conclusion

In conclusion, watermarking technology has emerged as a crucial tool in the ongoing battle against video piracy. By embedding unique and imperceptible markers within video content, watermarking enables content owners and distributors to track and identify instances of unauthorized copying, distribution, and consumption. This helps to deter potential pirates and facilitates the detection of illicit activities, ultimately safeguarding the rights and revenues of content creators and stakeholders.

However, while watermarking offers a promising solution, it's important to acknowledge that determined pirates might find ways to circumvent or remove watermarks. As technology evolves, so do the methods of piracy, making it a continuous challenge to stay one step ahead. Therefore, watermarking should be seen as part of a comprehensive anti-piracy strategy that includes legal measures, technical advancements, and user education.

The effectiveness of watermarking in piracy detection and avoidance lies not only in its technical capabilities but also in its integration with broader efforts to combat piracy. Collaboration among content creators, distributors, technology providers, and legal authorities is essential to create a robust ecosystem that discourages piracy and promotes legitimate content consumption.

In the ever-evolving landscape of digital media, watermarking remains a valuable tool to deter and identify instances of video piracy. Its role will likely continue to evolve alongside advancements in technology and the shifting tactics of pirates. By combining watermarking with other preventive measures, the industry can work toward a more secure and sustainable future for content creation and distribution.

References

[1] J.V. Bagade, Nilesh Khare, Nikhil Patil, and Abhijeet Kumar. A watermarking scheme with scrambled watermark for authentication of video, Jun 2014.

[2] Hao Ding, Ruixin Tao, Jing Sun, Jin Liu, Fan Zhang, Xiaoping Jiang, and Jianjin Li. A compressed-domain robust video watermarking against recompression attack. *IEEE Access*, PP:1–1, 02 2021.

[3] Abhinav Gupta and Phalguni Gupta. Watermarking of mpeg-4 videos. volume 3072, pages 746–752, 01 2004.

[4] Zehui Ke, Hailiang Huang, Yingwei Liang, Yi Ding, Xin Cheng, and Qingyao Wu. Robust video watermarking based on deep neural network and curriculum learning. In *2022 IEEE International Conference on e-Business Engineering (ICEBE)*, pages 80–85, 2022.

[5] Shaohui Liu, Feng Shi, Jiguang Wang, and Shengping Zhang. An improved spatial spread-spectrum video watermarking. *Intelligent Computation Technology and Automation, International Conference on*, 1:587–590, 05 2010.

[6] Manoj Pandey and Sushma Jaiswal. A comparative study of various digital image watermarking techniques: Specific to hybrid watermarking. *Recent Advances in Computer Science and Communications*, 08 2023.

[7] Khumanthem Singh, Thounaojam Singh, Oinam Imocha Singh, and Romen Taiyenjam. A blind video watermarking scheme based on scene change detection. *Indo-US Conference Workshop on CYBER SECURITY, CYBER CRIME CYBER FORENSICS*, 08 2009.

[8] Jing Sun, Xiaoping Jiang, Jin Liu, Fan Zhang, and Congying Li. An anti-recompression video watermarking algorithm in bitstream domain. *Tsinghua Science and Technology*, 26:154–162, 2021.

[9] Ta Minh Thanh and Pham Thanh Hiep. Frame background influence based invisible watermarking to visible video watermarking. In *2013 International Conference on Advanced Technologies for Communications (ATC 2013)*, pages 563–568, 2013.

[10] Xin Zhong and Frank Shih, 08 2019.