CREDENTIAL INTEGRATED PIRACY PREVENTION FOR OTT PLATFORMS

PROJECT REPORT

Submitted by

KASHYAP AJI (TKM19CS034)

SRIGANASH S (TKM19CS066)

SUBIN A M (TKM19CS067)

UMER BIN SHAH (TKM19CS069)

to

The APJ Abdul Kalam Technological University

In partial fulfilment of the requirements for the award of a B Tech Degree

in Computer Science and Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

TKM College of Engineering, Kollam

JUNE 2023

DECLARATION

We undersigned and declare that the project report on "**Credential integrated piracy prevention for OTT Platforms**" submitted for partial fulfilment of the requirements for the award of degree of Bachelor of technology of the APJ Abdul Kalam Technological University, Kerala is bonafide work done by us under the supervision of Dr Aneesh G Nath, Associate Professor of TKMCE. This submission represents our ideas in our own words and where ideas or words of others have been included, we have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Place: Kollam
Date: 23/06/2023

Kashyap Aji
Sriganash S
Subin A M
Umer Bin Shah

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

TKM COLLEGE OF ENGINEERING, KOLLAM,

KERALA, PIN 691005

CERTIFICATE

This is to certify that the Project Report entitled "**CREDENTIAL INTEGRATED PIRACY PREVENTION FOR OTT PLATFORMS**" is a bonafide record of the project developed by **KASHYAP AJI (TKM19CS034), SRIGANASH S (TKM19CS066), SUBIN AM (TKM19CS067) and UMER BIN SHAH(TKM19CS069)** of the eighth semester B-Tech (Computer Science and Engineering) in partial fulfilment of the academic requirements for the award of the Degree of Bachelor of Technology, in Computer Science and Engineering in the year 2022-2023 from TKM College of Engineering under APJ Abdul Kalam Technological University.

Project Coordinator

Prof. Nisa A K
Assistant Professor
Dept. of CSE

Head of the dept

Dr Dimple A. Shajahan
Head of Department
Dept. of CSE

Supervisor

Dr Aneesh G Nath
Associate Professor
Dept. of CSE

External Examiner

ACKNOWLEDGEMENT

We take this opportunity to express our deep sense of gratitude and sincere thanks to all who helped us to complete the project successfully.

We express our sincere gratitude to **Dr T. A. Shahul Hameed**, Principal, for providing us with all the necessary facilities and support for doing the project.

We are extremely grateful to **Prof. Nisa A.K.**, Project Coordinator and Asst. Professor, Department of Computer Science and Engineering, for her constructive guidance, advice, constant support and technical guidance provided throughout the making of this project. Without her intellectual support and apt suggestions at the perfect time, this project work would not be possible.

We want to express our profound gratitude to our project guide **Dr Aneesh G Nath**, Associate Professor, Department of Computer Science and Engineering, for his constructive guidance, advice, constant support and technical guidance provided throughout the making of this project.

We extend our immense gratitude to all Faculties and Technical Staffs in the Department of Computer Science and Engineering, for their help and necessary facilities to complete this work. Our humble gratitude and heartiest thanks also go to our parents and friends, who have supported and helped me on the course of this work.

Kashyap Aji
Sriganash S
Subin AM
Umer Bin Shah

ABSTRACT

The proliferation of over-the-top (OTT) platforms has brought convenient access to video content for users, but it has also resulted in increased piracy, causing significant revenue losses. To address this issue, a dual watermarking approach has been proposed, combining visible and invisible watermarking techniques. This approach aims to combat piracy on OTT platforms by covertly embedding user information as invisible watermarks in videos and introducing visible watermarks to deter screen recording. By embedding unique credentials in each user's video and constantly changing the position of the visible watermark, this model enhances accountability, strengthens copyright enforcement, and deters unauthorized distribution and screen recording piracy. Extensive testing on both invisible and visible watermarking modules has shown the high-quality performance of the watermarking technique, ensuring the integrity of the content and reinforcing the overall piracy prevention framework. The integration of these techniques in the "Credential Integrated Piracy Prevention for OTT Platforms" project presents a comprehensive and proactive approach to tackle piracy, safeguard revenue streams, and protect the rights of content creators, fostering a secure and sustainable environment for digital media consumption.

CONTENTS

Chapters **Page No.**

LIST OF FIGURES

LIST OF TABLES

ABBREVIATION

OTT	Over The Top
TV	Television
DRM	Digital Right Management
SVD	Singular Value Decomposition
DWT	Discrete Wavelet Transform
QIM	Quantization Index Modulation
DCT	Discrete Cosine Transform
PRNG	Pseudo Random Number Generation
AC	Alternate Current
UID	Unique Identifier
PSNR	Peak Signal to Noise Ratio
SSIM	Structural Similarity Index Measure
NCC	Normalized Cross Correlation
BER	Bit Error Rate
MSE	Mean Squared Error
PEO	Programme Educational Outcomes
PSO	Programme Specific Outcomes

CHAPTER 1
INTRODUCTION

1.1 Background

Over-the-top (OTT) platforms have experienced an unprecedented growth in recent years, fuelled by the increasing number of users consuming online content, particularly in the wake of the COVID-19 pandemic. The term "over-the-top" refers to the delivery of media content over the internet without the involvement of traditional broadcasting or cable networks. OTT platforms have revolutionized the way people access and consume entertainment, providing a wide range of content, including movies, TV shows, documentaries, and live events.

The proliferation of high-speed internet connectivity, advancements in streaming technologies, and the ubiquity of smartphones and connected devices have contributed to the surge in OTT platform usage. Users can now enjoy on-demand content anytime, anywhere, and on various devices, such as smart TVs, smartphones, tablets, and gaming consoles. This convenience and flexibility have made OTT platforms a popular choice for entertainment consumption.

The OTT market has become a vital element of the digital economy, attracting both established media giants and emerging players. According to industry reports, the global OTT market is expected to reach a projected revenue of $230 billion by 2028. This growth trajectory underscores the significance and potential of OTT platforms in the entertainment industry.

1.2 Problem Statement

The rapid growth of OTT platforms has brought forth a pressing concern for content protection, particularly with regards to piracy. Piracy poses significant challenges and risks to the OTT industry, content creators, and rights holders.

Firstly, piracy leads to substantial economic losses. Unauthorized distribution and consumption of copyrighted content result in revenue leakage and hinder the financial sustainability of content creators and OTT platforms. The availability of pirated content for free or at reduced prices undermines the revenue models that support content production and distribution. As a result, content creators may face difficulties in recouping their investments, leading to a potential decline in the quantity and quality of available content.

Secondly, piracy compromises the user experience and erodes trust in OTT platforms. Illegally obtained or low-quality pirated copies often lack the same level of audio-visual quality as legitimate content. Users may encounter issues such as distorted video and audio, poor streaming performance, or incomplete content. Such subpar experiences can negatively impact user satisfaction, discourage subscriptions, and even drive users towards illegal alternatives.

Furthermore, piracy undermines the principles of fair competition and intellectual property rights. Content creators invest significant resources in developing original and engaging content. Piracy not only devalues their intellectual property but also discourages innovation and creativity. When piracy goes unchecked, it creates an unfair playing field for legitimate content providers and hampers the growth and diversity of the OTT industry. While various methods, such as DRM and content encryption, have been employed to combat piracy on OTT platforms, these approaches have limitations. Pirates continue to find ways to circumvent DRM systems, decrypt encrypted content, and distribute unauthorized copies. Therefore, there is a need for innovative and robust techniques to prevent piracy effectively and protect the interests of content creators, OTT platforms, and consumers.

In this context, the problem addressed by this project is to develop a credential integrated piracy prevention system for OTT platforms. The goal is to propose a novel approach that combines watermarking techniques and credential integration to enhance content protection. By embedding unique credentials into the content accessed by each user, the system aims to deter piracy, track the source of unauthorized distribution, and ensure the security and integrity of digital content on OTT platforms.

1.3 Objectives

The primary objective of this project is to develop a comprehensive and effective system that addresses the challenges posed by piracy and enhances content protection on OTT platforms. The specific objectives of the project are as follows:

- **Develop a robust watermarking technique**: The project aims to design and implement an advanced watermarking technique specifically tailored for OTT platforms. The watermarking technique will enable the embedding of unique credentials into the accessed content without compromising its quality or usability.

- **Implement secure credential integration**: This will involve the development of authentication mechanisms and protocols to ensure that only authorized users can access and view the content. The integration of credentials will strengthen content protection by tying the user's identity to the watermarked content.

- **Enhance piracy detection and tracking**: The embedded watermarks will serve as digital fingerprints, enabling the identification of unauthorized copies and linking them back to the user responsible for the illegitimate release. By improving piracy detection and tracking capabilities, the system will act as a deterrent to potential pirates and provide valuable evidence for legal action.

- **Evaluate the effectiveness and performance of the proposed system**: The project will conduct extensive evaluations and performance tests to assess the effectiveness of the developed system in preventing piracy. This will involve watermark imperceptibility and robustness tests.

By achieving these objectives, the project aims to make significant contributions to the field of content protection on OTT platforms, mitigating the risks associated with piracy and safeguarding the interests of content creators, OTT platforms, and consumers alike.

1.4 Significance of the Project

The proposed technique of credential integrated piracy prevention using watermarking holds significant implications for the OTT industry. Firstly, it addresses the limitations of existing methods by providing an additional layer of security against piracy. Secondly, it offers a means to track and identify the source of pirated content, enabling legal actions against those responsible. This approach can act as a deterrent and significantly reduce the prevalence of piracy on OTT platforms. Additionally, content creators and platform operators can benefit from increased revenue and enhanced user trust, leading to a more sustainable and thriving OTT ecosystem.

1.5 Scope and Limitations

1.5.1 Scope

The scope of the project "Credential Integrated Piracy Prevention for OTT Platforms" encompasses the development and implementation of a comprehensive system for content protection on OTT platforms. The project focuses on the integration of watermarking techniques and user credentials to enhance piracy prevention and deter unauthorized distribution of digital content. The system aims to address the challenges posed by piracy, improve the user experience, and protect the interests of content creators and OTT platforms.

The project will involve the design and implementation of advanced watermarking techniques, the development of secure credential integration mechanisms, and the integration of piracy detection and tracking algorithms. Additionally, the project will establish a framework for comprehensive piracy prevention, including authentication protocols, legal enforcement strategies, and guidelines for industry adoption. The project's scope also includes the evaluation and assessment of the proposed system's effectiveness and performance. This will involve conducting experiments, simulations, and real-world testing to measure the accuracy of piracy detection, user authentication, and the overall efficacy of the system.

1.5.2 Limitations

While the project aims to develop an effective piracy prevention system for OTT platforms, it is essential to acknowledge certain limitations:

- **Legal and jurisdictional considerations**: The project focuses on technical solutions to prevent piracy, but legal and jurisdictional aspects may vary across different regions and countries. The effectiveness of legal enforcement strategies and the availability of appropriate legal frameworks for combating piracy may vary, which can impact the system's overall effectiveness.

- **User privacy concerns**: The project will involve the integration of user credentials into the watermarked content. While the system aims to ensure secure authentication, user privacy concerns must be addressed adequately. It is crucial to implement appropriate data protection measures and adhere to privacy regulations to safeguard user information.

- **Network infrastructure limitations**: The performance and effectiveness of the proposed system may depend on the network infrastructure available for content delivery. Issues such as network latency, bandwidth limitations, and content distribution networks' capabilities may impact the real-time implementation and scalability of the system.

- **System compatibility and integration**: The successful implementation of the piracy prevention system requires the cooperation and integration of OTT platforms and content distribution systems. Compatibility issues, technical constraints, and varying system architectures may present challenges during the integration process. The project will address these challenges within the scope of its capabilities.

- **Evolving piracy techniques**: Piracy methods and techniques are continually evolving, and determined pirates may find new ways to circumvent content protection measures. While the project aims to develop a robust system, it is essential to acknowledge that the system's effectiveness may be challenged by emerging piracy techniques and advancements in digital piracy.

Despite these limitations, the project strives to address the pressing concerns of content protection on OTT platforms by developing an innovative piracy prevention system. The project's outcomes and guidelines can serve as a valuable foundation for further research, industry adoption, and the continuous improvement of content protection mechanisms in the dynamic landscape of OTT platforms.

CHAPTER 2
LITERATURE SURVEY

2.1 Introduction

This chapter provides a comprehensive review of the existing literature on video watermarking techniques for piracy prevention on OTT platforms. The literature review aims to identify various approaches, methodologies, and algorithms proposed by researchers in this field. The review focuses on both blind and non-blind watermarking techniques, as well as compressed and uncompressed domain methods. The strengths and limitations of each approach are examined to highlight the gaps and opportunities for the proposed project.

2.2 Blind and Non-blind Watermarking Techniques

Video watermarking techniques can be broadly categorized into blind and non-blind techniques. Non-blind techniques require the original copy of the video sample during watermark extraction, while blind techniques do not. Divjot and Jindal **[4]** proposed a semi-blind video watermarking technique that combines SVD and DWT techniques. Their approach showed promising results against general noise and spatial attacks, but the study did not mention the resilience against geometric or collusion attacks. The majority of video watermarking techniques proposed in the past decade are blind, indicating their widespread adoption in the field.

2.3 Uncompressed Watermarking Techniques

Watermarking techniques can also be classified based on the point of embedding: compressed and uncompressed techniques. Uncompressed techniques involve embedding watermarks directly onto raw, uncompressed video frames. For instance, Liu et al. **[5]** proposed a robust watermarking algorithm based on Differential Energy and Quantization Index Modulation (QIM) for uncompressed video. Their algorithm utilizes modified low-frequency DEW and QIM for information embedding, with a focus on stable and high-amplitude low-frequency coefficients. However, their algorithm exhibits higher error rates in B-frames during compression. Compressed domain watermarking techniques embed watermarks directly into the compressed video stream. These techniques are suitable for real-time applications and are more tolerant of minor visual distortions. Satpute et al. **[11]** presented a compressed domain video watermarking technique that remains resistant to compression by utilizing 3D-DWT based video encoding and compression using the EZW algorithm.

2.4 Evaluation of Watermarking Techniques

The literature review encompasses a range of watermarking techniques proposed in recent studies. These techniques employ various methodologies, including SVD and DWT, scene-based feature extraction, temporal codes, complex maps, and transform domains such as DCT and contourlet. While many of these techniques demonstrate promising results in specific aspects, they may have limitations in terms of robustness against certain attacks, computational complexity, or resistance to specific compression formats. Some techniques show effectiveness against general noise and spatial attacks but fail to address geometric attacks or collusion attacks. These limitations highlight the need for further research and development to enhance the robustness and efficacy of video watermarking techniques for piracy prevention in OTT platforms.

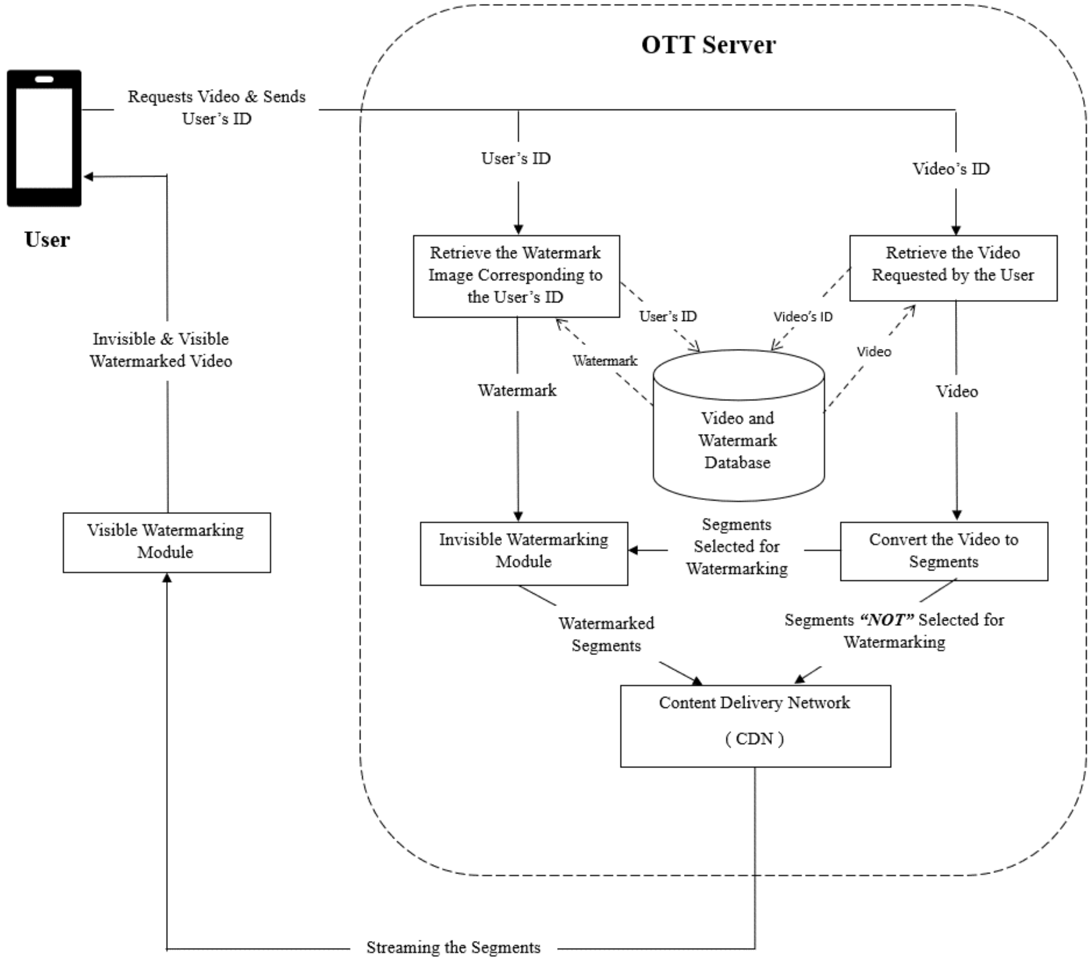
2.5 Summary

In summary, the literature review explores a wide range of video watermarking techniques for piracy prevention in OTT platforms. The review focuses on blind and non-blind approaches, as well as compressed and uncompressed domain techniques. The evaluated techniques demonstrate varying degrees of robustness against attacks, computational complexity, and resistance to compression formats. The findings from this review provide a solid foundation for the proposed Credential Integrated Piracy Prevention system, aiming to overcome the limitations and improve the effectiveness of existing watermarking techniques in protecting digital content on OTT platforms.

CHAPTER 3
PROJECT DESIGN

3.1 Introduction

This chapter presents the design of the Credential Integrated Piracy Prevention, which aims to protect video content from piracy in Over-the-Top (OTT) platforms. The design focuses on the integration of credentials and watermarking techniques to enhance the security and traceability of the content. This chapter outlines the workflow of the system, including the retrieval and application of user credentials, watermarking of video segments, and the usage of invisible and visible watermarks to track piracy sources and prevent unauthorized Cam cording.



OTT Server
Requests Video & Sends User's ID
User
User's ID
Video's ID
Retrieve the Watermark Image Corresponding to the User's ID
Retrieve the Video Requested by the User
User's ID
Video's ID
Watermark
Video
Video and Watermark Database
Watermark
Video
Invisible & Visible Watermarked Video
Visible Watermarking Module
Invisible Watermarking Module
Segments Selected for Watermarking
Convert the Video to Segments
Watermarked Segments
Segments "NOT" Selected for Watermarking
Content Delivery Network (CDN)
Streaming the Segments

Fig 3.1 Project Design

3.2 User Credential and Video Request Integration

When the user requests a video along with the video request, the user also sends their credentials to the OTT server. The integration of user credentials with the video request ensures a personalized and secure experience. The credentials serve as a unique identifier for the user and are used to retrieve their corresponding watermark.

3.3 Watermark Retrieval and Video Segments Selection

Upon receiving the video request and user credentials, the OTT server retrieves the watermark associated with the user. The watermark is retrieved using the provided credentials, ensuring that each user's content is uniquely identifiable. Simultaneously, the server selects the video segments corresponding to the user's request. These segments are determined based on the video metadata and user preferences.

3.4 Invisible Watermarking Module

The selected video segments are divided into two categories: segments to be watermarked and segments not required for watermarking. The segments not required for watermarking are streamed directly to the user while maintaining the video streaming experience. The segments to be watermarked are sent to the invisible watermarking module. This module applies the corresponding user watermark to the selected segments. The invisible watermarking technique ensures that the watermark is embedded seamlessly without affecting the visual quality of the video. The watermark serves as a unique identifier and can be used to trace the source of piracy if the video is illegally downloaded.

3.5 Watermarked Video Streaming

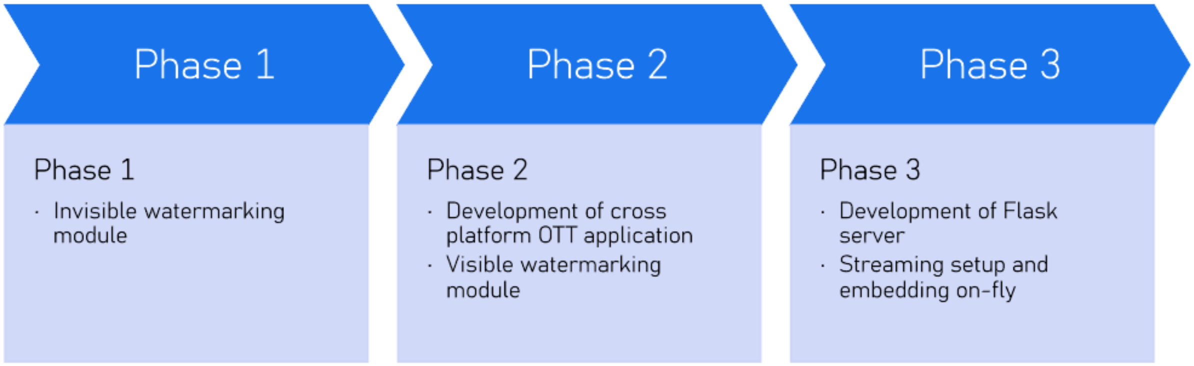
After the watermarking process is completed, the watermarked video segments are streamed to the user's device. The segments are streamed alongside the non-watermarked segments, ensuring a seamless playback experience for the user. Both the watermarked and non-watermarked segments are combined to provide a cohesive video experience. Upon reaching the user device, the watermarked video segments are further processed to include visible watermarks. The visible watermark is applied using the user's credentials, serving as an additional layer of protection against unauthorized Cam cording. The visible watermark acts as a deterrent, as any captured video containing the visible watermark can be traced back to the user who accessed the content.

3.6 Benefits of Invisible and Visible Watermarks

The usage of invisible watermarks in the video ensures that any illegal download of the content can be tracked back to its source, aiding in piracy detection and prevention. The invisible watermark serves as a covert identifier embedded within the video data. Simultaneously, the visible watermark applied using the user's credentials acts as a visible deterrent against unauthorized Cam cording. The presence of the visible watermark discourages individuals from recording the video, as the watermark can be used to identify the source of the recorded content.

3.7 Phases

In order to successfully implement the project design and attain its various objectives the project has to be divided into 3 phases.



Phase 1

Phase 2

Phase 3

Phase 1

- Invisible watermarking module

Phase 2

- Development of cross platform OTT application
- Visible watermarking module

Phase 3

- Development of Flask server
- Streaming setup and embedding on-fly

Fig 3.2 Different Phases of Project Implementation

CHAPTER 4
METHODOLOGY

4.1 Invisible Watermarking Module

1. Fractals

Chaotic systems are characterized by their sensitivity to initial conditions, where even a small change can lead to significantly different outcomes, rendering long-term behaviour unpredictable. However, amidst this unpredictability, certain systems exhibit recurring patterns and self-similarities at various scales, manifesting as distinct structures within the resulting patterns. These consistent patterns, known as strange attractors, maintain their structure regardless of the scale at which they are observed. Therefore, although the long-term behaviour of chaotic systems remains unpredictable, there are inherent patterns and structures that exhibit consistency and can be observed.

In this project, the selection of specific watermark locations, such as 4x4 boxes and channels, incorporates the utilization of the Newton chaotic map. An alternative approach could have been the use of pseudo-random number generators (PRNGs). However, employing PRNGs presents certain drawbacks, including the potential for generating repetitive patterns over time, which introduces security vulnerabilities. Additionally, PRNGs rely on a seed value to initiate number generation, and if an attacker obtains or guesses the seed value, they can predict the entire sequence of numbers generated by the PRNG. In contrast, fractals do not rely on a seed value and exhibit a self-similar structure that allows for a high degree of randomness without repetitive patterns. Furthermore, the patterns generated by fractals are intricate, complex, and difficult to replicate using PRNGs.

The Newton chaotic map applied in this project is based on previous research, specifically adapting the work presented in the reference paper “A blind video watermarking algorithm robust to lossy video compression attacks based on generalized Newton complex map and contourlet transform” **[2]**. By leveraging the principles of the Newton chaotic map, this project incorporates its unique properties to enhance the selection of watermark locations within digital media. The chaotic nature of the Newton map contributes to increased randomness, complexity, and uniqueness, which are vital aspects in an effective watermarking system.

In summary, fractals provide a framework to understand and observe the self-similar patterns exhibited by chaotic systems. The utilization of the Newton chaotic map in selecting watermark locations offers advantages over PRNGs, ensuring a higher degree of randomness without the need for a seed value. The complex and intricate patterns generated by fractals, combined with the principles of the Newton chaotic map, contribute to the development of a robust and secure watermarking technique. Building upon the existing research on the Newton chaotic map, this project aims to enhance copyright protection, establish ownership, and deter illegal distribution within the dynamic landscape of digital media.

2. Newton’s Chaotic Map

The classic Newton fractal, characterized by its two parameters - the initial parameter z0 and the control parameter α, presents certain limitations in its iterative behaviour. Upon repeated iterations, the fractal tends to converge towards positive and negative infinities, resulting in a single output value. This limitation hinders the generation of multiple numbers within the fractal.

To overcome this challenge, a complex folding procedure is introduced. The folding procedure involves mapping the output of the Newton fractal to a finite interval using a non-linear function. This process effectively "folds" the values back onto themselves, enabling a continuous and bounded output. As a result, the generating process generates more than one number, enhancing the variety and diversity of the output values.

By incorporating the complex folding procedure, the range of output values is confined within the interval [0,1]. This ensures that the generated numbers remain within a specific range, providing greater control and facilitating their utilization in various applications, such as watermarking. The introduction of the folding procedure resolves the issue of the classic Newton fractal converging to infinities and enables the generation of multiple numbers, thereby expanding the possibilities and versatility of the fractal in practical implementations.

In summary, the incorporation of a complex folding procedure enhances the capabilities of the classic Newton fractal. By mapping the fractal's output to a finite interval through a non-linear function, the folding procedure generates multiple numbers and constrains their values within a specific range. This advancement enables a broader range of applications, including watermarking, by providing greater control and diversity in the generated output.

The following equations represent the proposed polynomial functions of Newton's complex map:

$$\boldsymbol{f_1(Z_1) = Sin(Z_1)}\ , \tag{4.1}$$

$$\boldsymbol{f_2(Z_2) = Sin(Z_2)} \tag{4.2}$$

Along with these equations, the 2D model would be:

$$\boldsymbol{Z_1^{n+1} = Z_1^n - \alpha\,.\frac{f_1(Z_1^n).f_2(Z_2^n)}{f_1'(Z_1^n)}}\ , \tag{4.3}$$

$$\boldsymbol{Z_2^{n+1} = Z_2^n - \beta\,.\frac{f_2(Z_2^n).f_1(Z_1^n)}{f_2'(Z_2^n)}} \tag{4.4}$$

C-fold is the folding procedure utilized, Above equation with C-fold:

$$\boldsymbol{Z_1^{n+1} = \left[Z_1^n - \alpha\,.\frac{sin(Z_1^n).\mathrm{sin}(Z_2^n)}{\mathrm{co\ s}(Z_1^n)}\right] CFold\ 1}, \tag{4.5}$$

$$\boldsymbol{Z_2^{n+1} = \left[Z_2^n - \beta\,.\frac{sin(Z_2^n).\mathrm{sin}(Z_1^n)}{\mathrm{co\ s}(Z_2^n)}\right] CFold\ 1} \tag{4.6}$$

C-fold is calculated as:

$$\boldsymbol{Z\ CFold\ 1 = \left(Z^{Real}\ mod\ 1\right) + \left(Z^{Imag}\ mod\ 1\right) \mathrm{X}\ 1\mathrm{i}} \tag{4.7}$$

Proposed Complex map has six keys which includes [Z_1^{Real}, Z_1^{Imag}, Z_2^{Real}, Z_2^{Imag}] ∈ [0,1] and α, β ∈ [1,4] and has long term security and 2^{280} key length. This key space is large enough to resist brute-force attack. The proposed complex map introduces six key parameters, namely [Z_1^{Real}, Z_1^{Imag}, Z_2^{Real}, Z_2^{Imag}], all falling within the range of [0,1]. Additionally, the keys α and β are included, both ranging from 1 to 4. The utilization of these six keys, along with the specific range constraints, enhances the security and robustness of the complex map.

The chosen key length for this proposed complex map is 2280, ensuring a significant number of possible combinations within the key space. This extensive key space provides a high level of protection against brute-force attacks, where an attacker systematically attempts all possible combinations to gain unauthorized access. The large key space increases the computational complexity required to crack the encryption, significantly reducing the feasibility of such attacks.

3. Watermark Embedding

In the proposed scheme, the watermarking process is optimized by embedding the watermark only on select frames, determined by a pseudo-random number generator. This approach offers several advantages, including reduced computational complexity, increased robustness, and a higher level of security. By watermarking specific frames instead of all frames, computational resources are utilized more efficiently, resulting in improved performance and faster processing times.

To prepare the frames for watermarking, each frame is converted from the RGB color space to its corresponding YC_bC_r representation. The YC_bC_r colour model is preferred over RGB because its constituent components are less correlated. This means that any modification made to one component will have minimal impact on the others, allowing for superior visual quality preservation. This transformation ensures that the watermarking process has minimal perceptible impact on the overall visual experience.

A series of wavelet transformations are then applied to the selected frames. Initially, the Haar wavelet transformation is calculated on each channel, resulting in four components: the lower resolution approximation video frame (LL) and three detailed components - vertical (LH), diagonal (HH), and horizontal (HL). These wavelet components capture different aspects of the frame's information and contribute to the overall embedding process. The wavelet transformation can be performed at multiple levels, where each level provides more stability but reduces the available area for watermark embedding.

To further enhance the quality and compression capabilities, a second wavelet transformation using the Daubechies 16 wavelet is applied specifically on the LL component. The Daubechies wavelet has the ability to capture both local and global features in the data and offers a high level of compression while preserving important information. These wavelets have a compact support, meaning they are non-zero only within a finite interval, and exhibit localization in both the time and frequency domains.

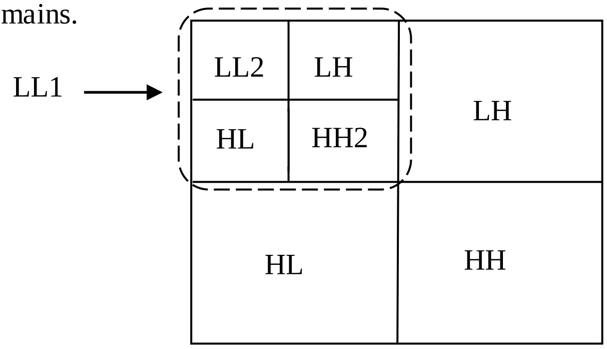


Fig 4.1 Selection of LL2 sub-band from LL1 sub-band

The resulting set of wavelet transformations, as shown in the provided figure, focuses on the LL2 sub-bands obtained from the last wavelet transformation. These sub-bands are carefully selected as optimal locations for embedding the watermark, ensuring maximum effectiveness and robustness. To determine the precise locations for watermark embedding, the output of the generated Newton complex map is utilized. The imaginary component (Z^{Imag}) of the complex map's output is employed to select the colour channel, while the real number components are used to identify 4x4 blocks within the frame. Subsequently, the discrete cosine transform (DCT) is applied to each 4x4 block, and the watermark is embedded by modifying the AC (alternating current) coefficients of the selected blocks. This approach ensures that the watermark is embedded in a controlled and imperceptible manner, minimizing the visual impact while maintaining its integrity for detection and identification purposes.

To these DCT blocks the watermarks are embedded using a hybrid algorithm specified below:

Watermark Embedding Algorithm

Input : n = number of randomly selected AC coefficients)

C = DCT applied 4x4 block

$W_{i,j}$ = Watermark at position (i,j)

α = Watermark Strength

$\beta = 2 * \alpha$

$\gamma = 3 * \alpha$

$\delta = 4 * \alpha$

$\varepsilon = 5 * \alpha$

Output : Watermarked block C

Steps :

```
1. if ($W_{i,j}$ == 1) then
    a. count = 0
    b. while (count < n) do
        i. if (($C_{i,j}$ mod $\delta$) $\leq \alpha$) then
            1. $C^{W}_{i,j} = C_{i,j}$ - ($C_{i,j}$ mod $\delta$) - $\alpha$
        ii. else
            1. $C^{W}_{i,j} = C_{i,j}$ - ($C_{i,j}$ mod $\delta$) + $\gamma$
        iii. endif
        iv. count = count + 1
    c. end while
2. elseif ($W_{i,j}$ == 0) then
    a. count = 0
    b. while (count < n) do
        i. if (($C_{i,j}$ mod  $\delta$) $\geq \gamma$) then
            1. $C^{W}_{i,j} = C_{i,j}$ - ($C_{i,j}$ mod $\delta$) + $\varepsilon$
        ii. else
            1. $C^{W}_{i,j} = C_{i,j}$ - ($C_{i,j}$ mod $\delta$) + $\alpha$
        iii. endif
        iv. count = count + 1
    c. end while
3. endif
```

After watermarking the DCT blocks an inverse DCT and a series of inverse DWT is performed to attain the Y, C_b and C_r components. These components are then merged and is converted back to the RGB image.

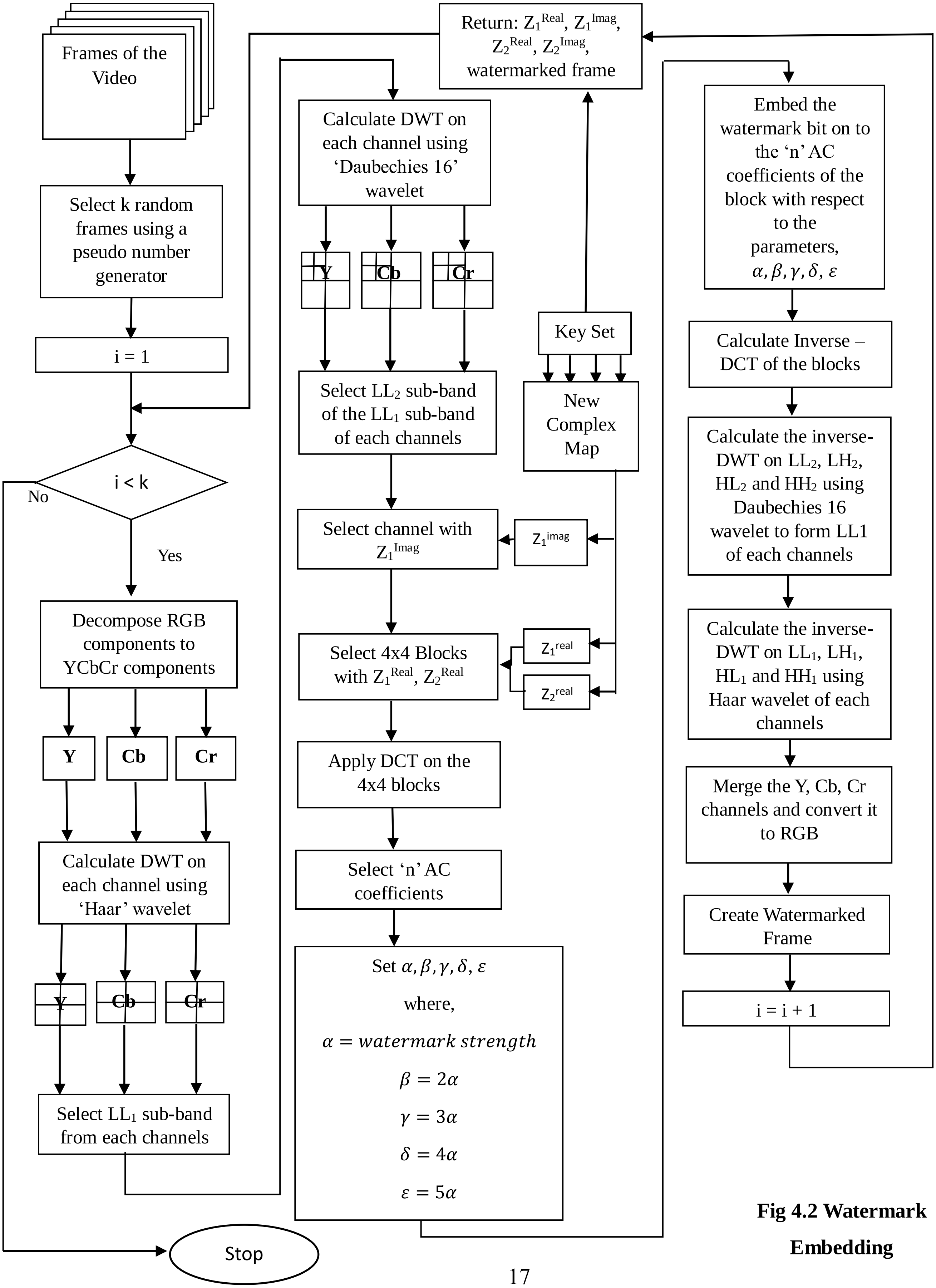

Frames of the Video
Select k random frames using a pseudo number generator
i = 1
i < k
No
Yes
Stop
Decompose RGB components to YCbCr components
Y
Cb
Cr
Calculate DWT on each channel using 'Haar' wavelet
Y
Cb
Cr
Select LL$_1$ sub-band from each channels
Calculate DWT on each channel using 'Daubechies 16' wavelet
Y
Cb
Cr
Select LL$_2$ sub-band of the LL$_1$ sub-band of each channels
Select channel with Z$_1^{Imag}$
Z$_1^{imag}$
Select 4x4 Blocks with Z$_1^{Real}$, Z$_2^{Real}$
Z$_1^{real}$
Z$_2^{real}$
Apply DCT on the 4x4 blocks
Select 'n' AC coefficients
Set $\alpha, \beta, \gamma, \delta, \varepsilon$
where,
$\alpha = watermark\ strength$
$\beta = 2\alpha$
$\gamma = 3\alpha$
$\delta = 4\alpha$
$\varepsilon = 5\alpha$
Key Set
New Complex Map
Return: Z$_1^{Real}$, Z$_1^{Imag}$, Z$_2^{Real}$, Z$_2^{Imag}$, watermarked frame
Embed the watermark bit on to the 'n' AC coefficients of the block with respect to the parameters, $\alpha, \beta, \gamma, \delta, \varepsilon$
Calculate Inverse – DCT of the blocks
Calculate the inverse-DWT on LL$_2$, LH$_2$, HL$_2$ and HH$_2$ using Daubechies 16 wavelet to form LL1 of each channels
Calculate the inverse-DWT on LL$_1$, LH$_1$, HL$_1$ and HH$_1$ using Haar wavelet of each channels
Merge the Y, Cb, Cr channels and convert it to RGB
Create Watermarked Frame
i = i + 1

Fig 4.2 Watermark Embedding

Overall, the proposed scheme integrates a series of steps, including selective frame watermarking, YC_bC_r conversion, wavelet transformations, and precise block selection using the Newton complex map. These techniques collectively enhance the efficiency, security, and visual quality preservation of the watermarking process.

4. Watermark Extraction

Extraction follows the same procedure as in embedding up to the point of obtaining 4x4 DCT blocks (Two DWT decomposition and application of Newton's chaotic complex map).The following algorithm is then applied on n AC coefficients of selected 4x4 to retrieve the watermark.

Watermark Extracting Algorithm

```
Input : n = number of randomly selected AC coefficients)
        C = DCT applied watermarked 4x4 block
        $\alpha$ = Watermark Strength
        $\beta$ = 2 * $\alpha$
        $\gamma$ = 3 * $\alpha$
        $\delta$ = 4 * $\alpha$
        $\varepsilon$ = 5 * $\alpha$
Output :
        $W_{i,j}$ = Watermark at position (i,j)
Steps :
    1. while (count < n) do
        a. if (($C_{i,j}$ mod $\delta$) $>$ $\beta$) then
            i. $W_{i,j}$ = 1
        b. else
            i. $W_{i,j}$ = 0
        c. endif
    2. count = count + 1
    3. end while
```

Using the algorithm all the watermark bits are extracted from the frame. Thus, if there are k frames to which we applied the watermark to, then k watermarks will be returned by the extracting function. We could apply an arithmetic mean to all these watermarks to extract the final watermark.

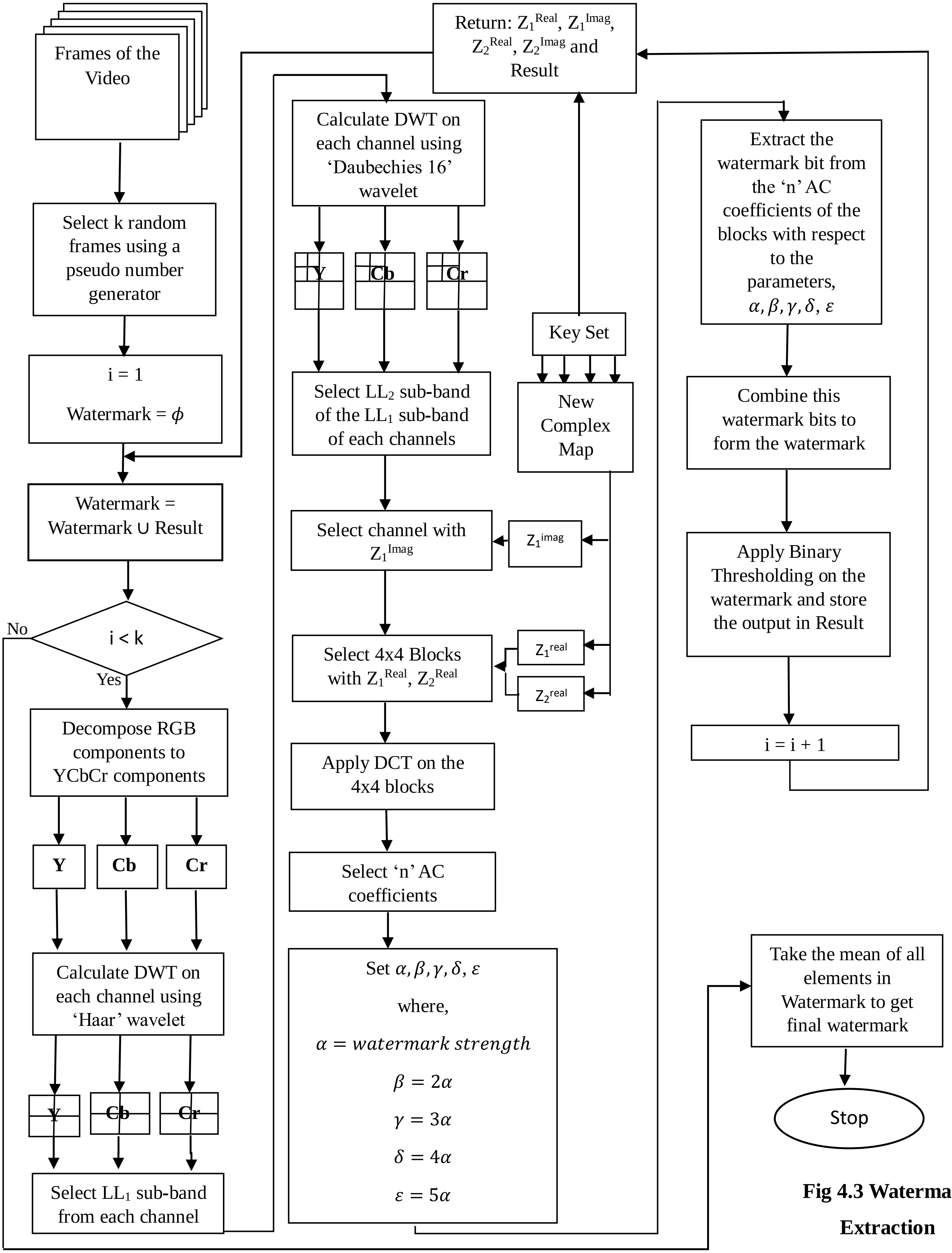

Frames of the Video
Select k random frames using a pseudo number generator
i = 1
Watermark = ϕ
Watermark = Watermark ∪ Result
i < k
No
Yes
Decompose RGB components to YCbCr components
Y
Cb
Cr
Calculate DWT on each channel using 'Haar' wavelet
Y
Cb
Cr
Select LL₁ sub-band from each channel
Calculate DWT on each channel using 'Daubechies 16' wavelet
Y
Cb
Cr
Select LL₂ sub-band of the LL₁ sub-band of each channels
Select channel with Z_1^{Imag}
Z_1^{imag}
Select 4x4 Blocks with Z_1^{Real}, Z_2^{Real}
Z_1^{real}
Z_2^{real}
Apply DCT on the 4x4 blocks
Select 'n' AC coefficients
Set $\alpha, \beta, \gamma, \delta, \varepsilon$
where,
$\alpha = watermark\ strength$
$\beta = 2\alpha$
$\gamma = 3\alpha$
$\delta = 4\alpha$
$\varepsilon = 5\alpha$
Return: Z_1^{Real}, Z_1^{Imag}, Z_2^{Real}, Z_2^{Imag} and Result
Key Set
New Complex Map
Extract the watermark bit from the 'n' AC coefficients of the blocks with respect to the parameters, $\alpha, \beta, \gamma, \delta, \varepsilon$
Combine this watermark bits to form the watermark
Apply Binary Thresholding on the watermark and store the output in Result
i = i + 1
Take the mean of all elements in Watermark to get final watermark
Stop

Fig 4.3 Watermark Extraction

4.2 Development of Cross-Platform OTT Application

Credstream is a cutting-edge streaming application developed using the Flutter framework, designed to provide users with a seamless and enjoyable experience accessing a wide range of exclusive and original content. Operating on a subscription-based model, Credstream offers a diverse collection of movies, TV shows, documentaries, and more, all conveniently available at users' fingertips.

With its sleek and user-friendly interface, Credstream ensures effortless navigation and discovery of content. Powered by the Flutter framework, the application delivers a visually appealing and responsive interface, enhancing user satisfaction and engagement. Users can easily explore the extensive content library, discover new releases, and find their favourite shows with just a few taps.

One of the standout features of Credstream is its cross-platform compatibility, made possible by leveraging the flexibility of the Flutter framework. Whether users prefer to stream on their smartphones, tablets, or smart TVs, Credstream provides a consistent and immersive streaming experience across different devices. This versatility allows users to enjoy their favourite content on the go or in the comfort of their own homes, adapting to their preferences and lifestyles.

Furthermore, Credstream offers the convenience of offline viewing, enabling users to download their desired content and watch it later, even without an internet connection. This feature is particularly beneficial for users with limited internet connectivity or those who want to save on data usage. By allowing offline viewing, Credstream enhances the flexibility and accessibility of its content, ensuring that users can enjoy their favourite shows and movies on their own terms.

In summary, Credstream, developed using the powerful Flutter framework, is a subscription-based streaming application that provides users with a seamless and engaging experience. Its user-friendly interface, cross-platform compatibility, and offline viewing feature make it a comprehensive solution for accessing exclusive and original content across various devices.

4.3 Visible Watermarking Module

In the context of protecting video content on OTT platforms, both invisible watermarking and visible watermarking techniques are employed to enhance the overall security measures. While invisible watermarking provides a covert means of embedding ownership information, visible watermarking serves as an additional deterrent against unauthorized recording or piracy attempts.

The implementation of visible watermarking becomes crucial in scenarios where external recording devices, such as cameras, may fail to capture the invisible watermark. By overlaying a visible watermark on the client-side video player, an extra layer of protection is added to prevent unauthorized duplication or distribution of the content.

To ensure minimal interference with the viewer's experience and the underlying invisible watermark, the visible watermark is designed to be as transparent as possible. This transparency allows the viewer to enjoy the content without significant distraction or degradation in visual quality. By carefully adjusting the transparency level, the visible watermark becomes subtly embedded within the video, maintaining a balance between visibility and unobtrusiveness.

Moreover, to further enhance the security and deter potential attackers, the position of the visible watermark dynamically changes over time. This dynamic positioning is achieved by leveraging a random number generator, which generates unpredictable coordinates for the watermark's placement. The use of a random number generator ensures that the visible watermark is not static and cannot be easily removed or cropped out by malicious entities.

Importantly, the visible watermark is added as a separate layer on top of the video content, ensuring that it does not interfere with the underlying video quality. This approach guarantees that the visible watermark remains visually distinct while preserving the original video's integrity and clarity.

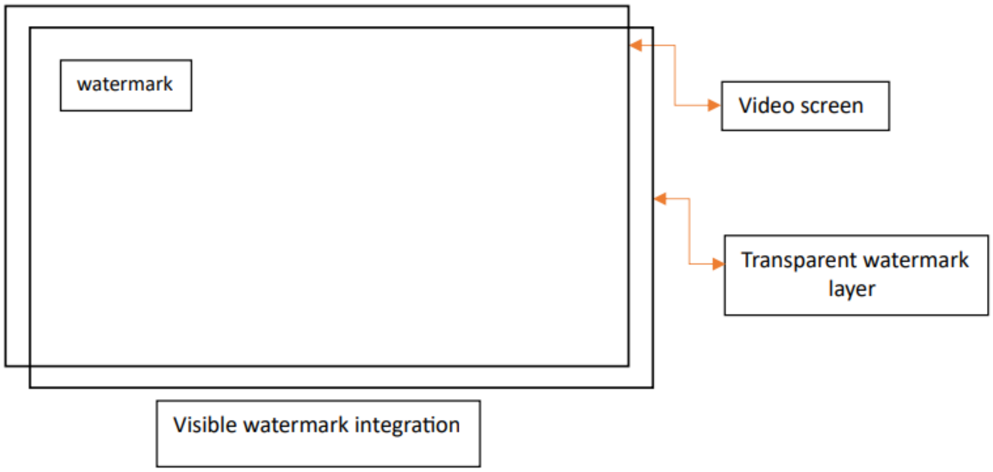


Fig 4.4 Visible Watermark Integration

4.4 Streaming Setup

One of the primary requirements in a streaming setup is to minimize buffering to ensure a seamless user viewing experience. Considering that our watermarking technique is primarily intended for uncompressed applications, the conventional approach would be to embed the watermark at the moment of receiving a request for video content, recompress it upon completion, and then stream it. However, this approach would result in a significant waiting period from the point of request to the readiness of the stream.

To address this issue, an alternative approach is adopted, which involves segmenting the entire video and embedding the watermark in real-time as the user seeks a particular portion or based on their viewing progress. This approach divides the streaming task into two main steps: pre-selection of segments to be embedded and streaming and embedding on the fly.

1. **Pre-selection of Segments**:

   To minimize the impact on the viewing experience caused by the time lag induced during playback due to watermarking on the fly, segments to be embedded should be selected in a manner that maximizes the gap between consecutive segments. This selection process follows a specific algorithm to ensure the criteria of minimum gap between consecutive segments is upheld.

Algorithm

```
List                                    //contains all segment numbers
Result= $\Phi$

Procedure Check(a, b)
    1. if mean( a, b) -- a >=3 &&  b -- mean( a, b )
            a. return true
    2. else
            b. return false

Procedure  Seg
    1. Let Q be a dictionary
    2. Insert first and last element of List as key and difference between two as value into the
       dictionary
    3. count=0
```

```
4. while $Q \neq \Phi$ & $count \neq k$
5. SORT(Q)                    //based on value
6. {a,b}=POP(q)
7. if check(a,b) then
        a. Result = Result ∪ {mean(a,b)}
        b. Q.add( { a , mean(a,b) } , mean(a,b) – a  )
        c. Q.add( {mean(a,b) , b } , b -- mean(a,b)  )
        d. Increment count
```

The algorithm begins with a list containing all segment numbers, where each segment is of equal length and assigned a number based on its sequence in the original video content. Approximately 25% of these segments are selected for watermark embedding.

The algorithm's objective is to maximize the average gap between selected segments, ensuring a minimum gap between consecutive segments. The algorithm uses a dictionary data structure to pair segments and identifies two segments with the maximum gap between them as the extremities of the list. It then proceeds to identify three segments: the two extreme segments and the segment closest to the mean of their segment numbers. This process is iterated until all possibilities of segment selection are exhausted or until the required number of segments have been selected. During each iteration, the algorithm checks if the segment should be selected based on the minimum gap required and adds it to the result set if the criteria are met.

2. **Streaming and Embedding on the Fly**:

In this step, the selected segments for watermark embedding, along with other common segments, are stored in separate directories. The segments to be embedded typically account for approximately 25 to 30% of the total number of segments, and the exact number may vary depending on the segment length and the time required to embed the watermark.

Upon receiving a request from the client, the streaming system checks both the common segment directory and a directory named after the requesting client's unique identifier (UID) for the requested segment. If the segment is found in either directory, it is relayed to the client. However, if the segment is not found, a watermarked copy of the requested segment is generated on the fly. The watermarked segment is then stored in the directory named after the UID of the requesting client and subsequently relayed back to the client for seamless streaming.

Once the user session ends, all the files in the user-specific directory are deleted, ensuring that the system maintains efficiency and does not accumulate unnecessary data.

By employing this segmented streaming and on-the-fly watermark embedding approach, the streaming setup achieves reduced buffering, increased robustness, and higher levels of security. The intelligent selection of segments for watermarking, along with the real-time generation of watermarked segments, optimizes the overall streaming experience while ensuring the protection of digital content.

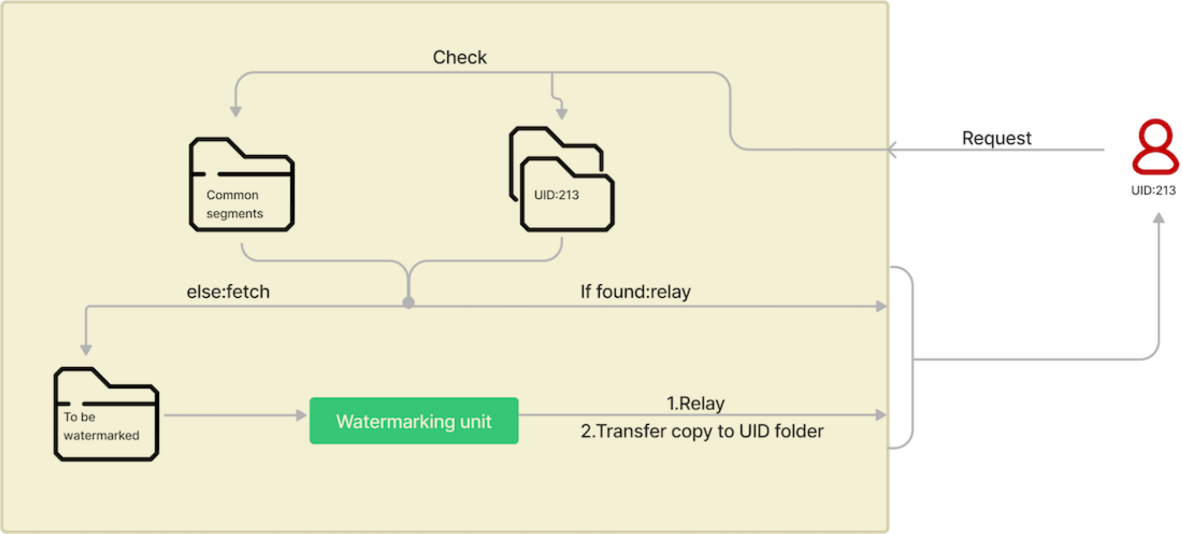


Fig 4.5 Streaming Setup

4.5 OTT Server

The OTT server in this project employs a database model consisting of three main entities: user, video, and watermark. Each user has their own watermark associated with their account, ensuring personalized and secure watermarking for content protection.

The server utilizes the Flask framework's @app.route functionality to serve the required URLs for API functionality. The server's responses are JSONified to facilitate seamless integration with the Flutter application.

The OTT server offers a range of major functionalities to enhance user experience. These functionalities include user registration, login, and logout capabilities, ensuring secure access to the platform. The server also provides the necessary functionality to serve video segments with streaming capabilities, while simultaneously embedding watermarks in real-time to protect the content from unauthorized distribution. Additionally, the server serves video metadata and thumbnails, enriching the user interface with relevant information about the available content.

In addition to the functionalities designed specifically for the Flutter application, the server also offers several other functionalities. These include the ability to add video metadata and thumbnails, ensuring comprehensive information about each video. Furthermore, the server incorporates video file segmentation and classification, distinguishing between common and open segments. This classification allows for better organization and management of the video files.

To maintain data privacy and optimize storage, the server automatically deletes user-specific watermarked segments after a specific period. In this case, the embedded segments are deleted after 5 hours, ensuring that no residual content remains accessible. The server also includes functionality for watermark extraction and matching, allowing for the verification and authentication of watermarked content.

CHAPTER 5
EXPERIMENTAL RESULTS

5.1 Invisible Watermarking Module

To verify the effectiveness and performance of the proposed invisible watermarking model several experiments were conducted. As part of several experiments a database of 17 videos was created. The experiment is performed on Intel Core i5 CPU under Windows 10. These videos can be accessed from media.xiph.org/video/derf/. The videos were commonly of 3 different standard resolution formats: 352x288, 1280x720, 1920x1080, thus emulating various viewing bandwidth options available on streaming platforms. The size of the watermark tested out is 32x32. The value of watermark strength α is chosen as 20 to ensure a perfect balance between watermark strength, visual quality and robustness against compression.

1. Imperceptibility Test

The imperceptibility of the invisible watermarking model in this project was evaluated using various metrics, including:

- Peak-Signal-to-Noise-Ratio (PSNR)
- Structure-Similarity-Index-Measure (SSIM)
- Normalized Cross Correlation (NCC)
- Bit Error Rate (BER).

PSNR is a measure of the quality of the watermarked image, calculated by comparing the original image with the watermarked image. It quantifies the degradation of image quality after watermarking, with higher PSNR values indicating better image quality.

$$\boldsymbol{PSNR = 10log_{10}\left(\frac{MAX_{Ov}^{2}}{MSE}\right)} \qquad (5.1)$$

Where MAX_{Ov} is the maximum possible pixel value between the frame of original video and the frame of watermarked video. Mean square error (MSE) is defined by:

$$\boldsymbol{MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}[O_v(i,j) - W_v(i,j)]^2} \qquad (5.2)$$

SSIM, on the other hand, measures the similarity between the watermarked image and the original image, considering luminance, contrast, and structure. Higher SSIM values indicate higher image quality.

$$\boldsymbol{SSIM(O_v, W_v)} = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \qquad (5.3)$$

The NCC metric assesses the visual quality of the extracted watermark by calculating the similarity between the original watermark image and the decoded watermark image. A high NCC value indicates a well-embedded watermark in the image.

$$\text{NCC} = \frac{\sum_i \sum_j W_{ij}\hat{W}_{ij}}{\sum_i \sum_j (W_{ij})^2} \qquad (5.4)$$

Additionally, the Bit Error Rate (BER) measures the accuracy of watermark detection and the robustness of the watermark against various attacks. It calculates the ratio of incorrect bits in the extracted watermark to the total number of bits, with lower BER values indicating higher watermark quality.

$$BER(W, EW) = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j) \oplus EW(i,j)}{m \times n} \times 100 \qquad (5.5)$$

Imperceptibility Test					
Video	**Resolution**	**PSNR**	**SSIM**	**NCC**	**BER**
City	352x288	34.36035	0.94522	1	0
Crew	352x288	34.15286	0.90954	1	0
Deadline	352x288	34.29562	0.96067	1	0
Harbour	352x288	30.57647	0.95269	0.99	1.95E-07
Ice	352x288	36.49662	0.94444	1	1.50E-08
Paris	352x288	27.94705	0.9575	1	0
Soccer	352x288	34.84986	0.92929	1	4.51E-08
Students	352x288	35.99684	0.95649	1	0
Wash_DC	352x288	36.19115	0.976704	1	0
Ducks	1280x720	29.11286	0.89902	1	4.51E-08
Johny	1280x720	38.20799	0.952191	1	0.00
Four People	1280x720	37.96607	0.95451	1	0
Vidyo1	1280x720	38.68298	0.963791	1	0
River Bed	1920x1080	34.60617	0.90853	1	9.01E-08
Rush Hour	1920x1080	38.46212	0.94178	1	0.00
Station	1920x1080	38.02774	0.948825	1	0
Sunflower	1920x1080	39.08013	0.969613	1	0
Average		35.236052	0.9453414	0.9994118	2.3E-08

Table 5.1 Result of Imperceptibility Test

The table above presents the results of the imperceptibility test using PSNR, SSIM, NCC, and BER metrics. The PSNR values show an average range of 35, which is considered sufficient for a good visual experience. The overall PSNR and SSIM results demonstrate the ability of the proposed method to achieve high visual quality. The NCC values remain consistently at 1 for all video samples, except for the "Harbour" sample. Furthermore, the BER values remain close to 0, indicating the quality of watermark preservation after extraction.

2. Robustness Against Compression

The proposed algorithm's robustness against various types of lossy compression techniques, such as MPEG4, MPEG2, ASF, H.264, etc., was evaluated to assess its performance under different compression scenarios. The evaluation focused on measuring the normalized cross correlation (NCC) and bit error rate (BER) between the original watermark and the extracted watermark after applying the compression.

The NCC value indicates the similarity between the original watermark and the extracted watermark, while the BER value reflects the accuracy of watermark detection and the robustness of the watermark against compression-induced errors. Higher NCC values and lower BER values indicate better performance and increased resistance to compression.

Compression	BER	NCC
ASF	1.20E-07	0.995734
DVD	4.22E-06	0.827593
FLV	3.89E-08	0.998618
H264	2.60E-07	0.991041
MJPEG	3.80E-08	0.998645
MKV	1.19E-07	0.995757
MPEG4	2.60E-07	0.991041
MPEG1	5.30E-08	0.998125
MPEG2	5.30E-08	0.998125
MXF	5.04E-08	0.998205
WMV	1.20E-07	0.995734
XVID	3.80E-08	0.998645

Table 5.2 Result of Compression Attacks

The table presents the NCC and BER results between the original watermark and the extracted watermarks, showcasing the performance of the proposed method under different compression techniques.

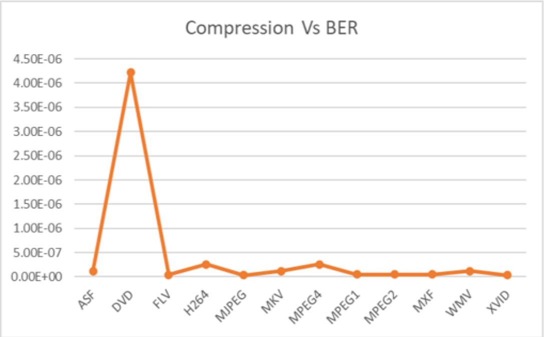


Fig 5.1 Compression Vs BER

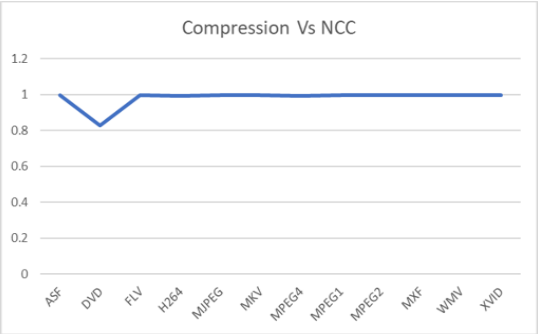


Fig 5.2 Compression Vs NCC

The results clearly demonstrate that the proposed video watermarking method exhibits high resistance against most lossy compression techniques. The method performs exceptionally well under compression formats such as MPEG1, MPEG2, MXF, XVID, MJPEG, and FLV, as evidenced by consistent NCC values of 1 and BER values close to 0. The consistently high numerical values for NCC, averaging above 0.99, and the low values for BER, averaging nearly 0, provide compelling evidence of the reliability and effectiveness of the watermarking method used.

3. Result of Invisible Watermarking Module

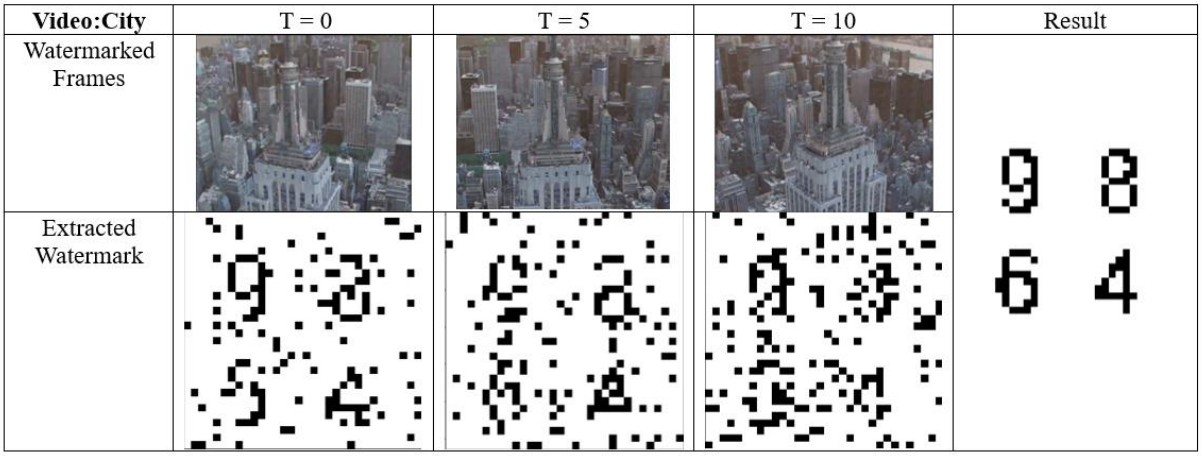


Fig 5.3 City Video after Watermark Embedding and Extraction

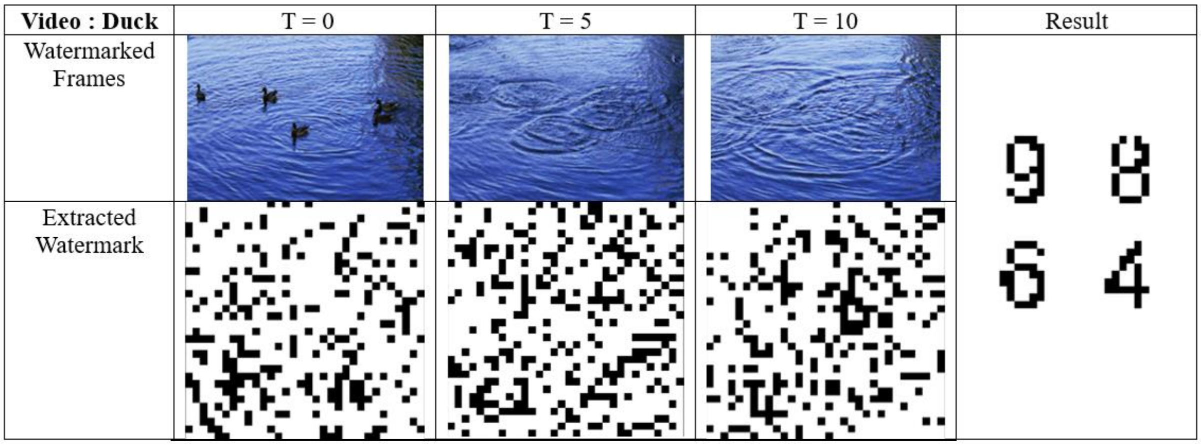


Fig 5.4 Duck Video after Watermark Embedding and Extraction

5.2 CredStream: The Cross Platform OTT Application

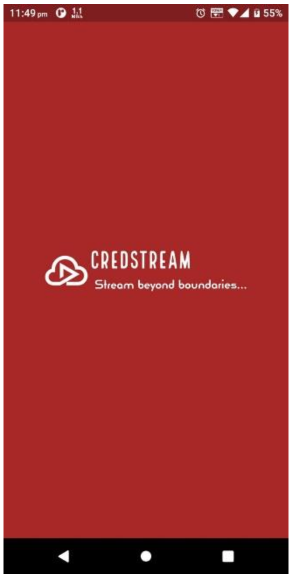


Fig 5.5 Launch Screen

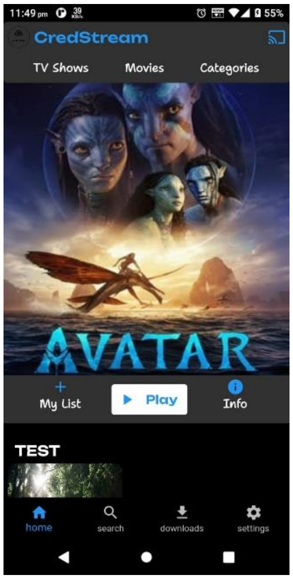


Fig 5.6 Home Screen

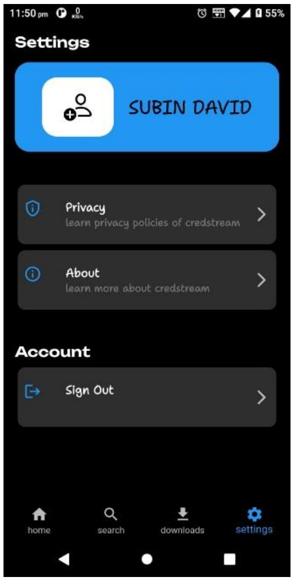
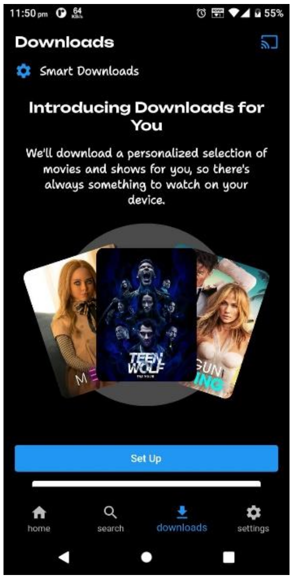


Fig 5.7 Profile



Introducing Downloads for You

We'll download a personalized selection of movies and shows for you, so there's always something to watch on your device.

Fig 5.8 Download Screen

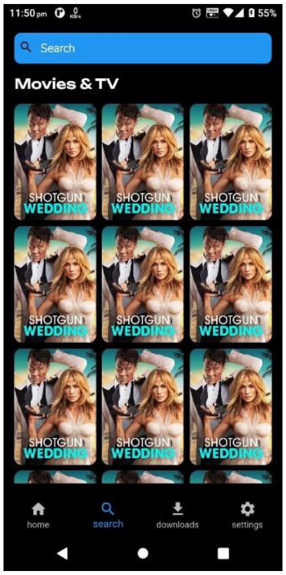


Fig 5.9 Search Screen

5.3 Visible Watermarking Module

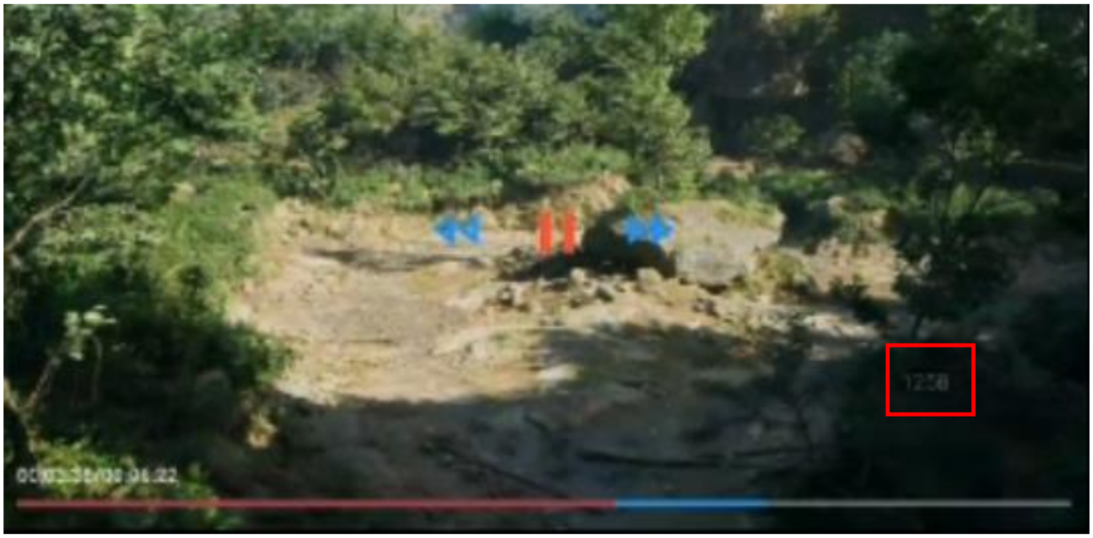


Fig 5.10 Visibly Watermarked Video

The visible watermark implemented in this project offers a highly effective second level of security against cam-cording theft. By incorporating the watermark at the client side, not only is the protection of video content ensured, but it also contributes to reducing the server load, thereby enhancing overall system performance. The watermark's independence from the video content is a critical aspect that plays a pivotal role in maintaining a seamless user experience. This means that viewers can enjoy the content without any disruptions or degradation caused by the presence of the watermark.

One of the remarkable features of the implemented watermark is its dynamic nature, which serves as a formidable defence against geometric attacks. Geometric attacks include flipping, cropping, scaling, and translating, among others. By incorporating dynamic watermarking, unauthorized individuals face significant challenges when attempting to tamper with or remove the watermark without compromising the video's integrity. This robustness ensures that the video content remains protected against unauthorized distribution and piracy.

The effectiveness and reliability of the implemented visible watermark are further exemplified by the notable results achieved. These results confirm the watermark's ability to deter unauthorized distribution, safeguard valuable video content, and ultimately improve user satisfaction. The visible watermark serves as an effective deterrent against cam-cording theft, acting as a visible indicator of ownership and discouraging potential infringers.

By implementing this visible watermarking technique, the project not only enhances the security measures surrounding video content but also reinforces the trust and confidence of content creators and distributors. The protection provided by the watermark contributes to maintaining the value and exclusivity of the content, ultimately benefiting both content owners and end-users.

Overall, the implemented visible watermark proves to be a valuable addition to the project's security measures, ensuring the integrity and protection of video content, minimizing unauthorized distribution, and enhancing the overall user experience.

CHAPTER 6
CONCLUSION

In this project, we have successfully implemented a dual watermarking scheme using both invisible and visible watermarking modules to combat piracy of OTT videos. The invisible watermarking module plays a crucial role in preventing unauthorized distribution and tracking down potential infringers. By watermarking the requested video with the user's unique watermark or credentials before streaming, any attempt to download the video in an unlawful manner will result in the pirate obtaining a copy that carries their own watermark. This method acts as a powerful deterrent, as it becomes much easier to trace the source of unauthorized distribution.

Additionally, the visible watermarking module adds an extra layer of protection by overlaying the user's watermark on top of the requested video. This technique serves as an effective measure against illegal screen recordings, as the user's watermark is clearly visible throughout the entire video. Any unauthorized sharing or distribution of such a watermarked video would immediately expose the source of piracy, discouraging potential infringers and protecting the content owner's rights.

Furthermore, we conducted tests to evaluate the performance of the invisible and visible watermarking modules. For the invisible watermarking module tests were conducted on imperceptibility and robustness against compression under various compression scenarios. The results of these tests confirmed the effectiveness of the invisible watermarking module in maintaining the integrity of the watermark while maintaining the video's quality. The examination performed on the visible watermarking module has demonstrated that the watermark does not introduce any visual disruptions, and the placement of the watermark varies dynamically over time.

Overall, the combination of invisible and visible watermarking modules has proven to be a valuable approach in preventing piracy of OTT videos. The dual watermarking scheme provides a robust solution that safeguards content ownership and acts as a deterrent against unauthorized distribution.

REFERENCE

[1] Karmakar, A., Phadikar, A., Phadikar, B. S., & Maity, G. K. (2016). A blind video watermarking scheme resistant to rotation and collusion attacks. Journal of King Saud University - Computer and Information Sciences, 28(2), 199–210. https://doi.org/10.1016/j.jksuci.2014.06.019

[2] Barani, M. J., Ayubi, P., Valandar, M. Y., & Irani, B. Y. (2020). A blind video watermarking algorithm robust to lossy video compression attacks based on generalized Newton complex map and contourlet transform. Multimedia Tools and Applications, 79(3–4), 2127–2159. https://doi.org/10.1007/s11042-019-08225-5

[3] Liu, Q., Yang, S., Liu, J., Xiong, P., & Zhou, M. (2020). A discrete wavelet transform and singular value decomposition-based digital video watermark method. Applied Mathematical Modelling, 85, 273–293. https://doi.org/10.1016/j.apm.2020.04.015

[4] Thind, D. K., & Jindal, S. (2015). A Semi Blind DWT-SVD Video Watermarking. *Procedia Computer Science*, *46*, 1661–1667. https://doi.org/10.1016/j.procs.2015.02.104

[5] Liu, Z., Li, Q., Guan, S., & Peng, X. (2009b). *A Robust Watermarking Algorithm Based on Differential Energy and QIM for Uncompressed Video*. https://doi.org/10.1109/iih-msp.2009.273

[6] Tokar, T., Kanocz, T., & Levicky, D. (2009). *Digital watermarking of uncompressed video in spatial domain*. https://doi.org/10.1109/radioelek.2009.5158780

[7] Goel, B., & Agarwal, C. (2013). *An optimized un-compressed video watermarking scheme based on SVD and DWT*. https://doi.org/10.1109/ic3.2013.6612210

[8] Ramkumar, G., & Arivazhagan, N. (2014). *Uncompressed digital video watermarking using stationary wavelet transform*. https://doi.org/10.1109/icaccct.2014.7019299

[9] Velazquez-Garcia, L., Cedillo-Hernandez, A., Cedillo-Hernandez, M., Nakano-Miyatake, M., & Perez-Meana, H. (2021). Imperceptible–visible watermarking for copyright protection of digital videos based on temporal codes. *Signal Processing: Image Communication*, *102*, 116593. https://doi.org/10.1016/j.image.2021.116593

[10] Jung, H., Lee, Y., & Lee, S. Y. (2004). RST-Resilient Video Watermarking Using Scene-Based Feature Extraction. *EURASIP Journal on Advances in Signal Processing*, *2004*(14). https://doi.org/10.1155/s1110865704405046

[11] Satpute, V. R., Kadu, S., & Naveen, C. (2016). *Compressed domain video watermarking using EZW and chaos*. https://doi.org/10.1109/tencon.2016.7848615

[12] Lu, C., Chen, J., & Fan, K. (2005). Real-time frame-dependent video watermarking in VLC domain. *Signal Processing-image Communication*, *20*(7), 624–642. https://doi.org/10.1016/j.image.2005.03.012

[13] Ding, H., Tao, R., Sun, J., Liu, J., Zhang, F., Jiang, X., & Li, J. (2021). A Compressed-Domain Robust Video Watermarking Against Recompression Attack. *IEEE Access*, *9*, 35324–35337. https://doi.org/10.1109/access.2021.3062468

[14] Mansouri, A., & Mahmoudi-Aznaveh, A. (2019). Toward a secure video watermarking in compressed domain. *Journal of Information Security and Applications*, *48*, 102370. https://doi.org/10.1016/j.jisa.2019.102370

[15] Sun, Y., Wang, J., Huang, H., & Chen, Q. (2021). Research on scalable video watermarking algorithm based on H.264 compressed domain. *Optik*, *227*, 165911. https://doi.org/10.1016/j.ijleo.2020.165911

[16] Lee, M., Im, D., Lee, H., Kim, K. H., & Lee, H. (2012). Real-time video watermarking system on the compressed domain for high-definition video contents: Practical issues. *Digital Signal Processing*, *22*(1), 190–198. https://doi.org/10.1016/j.dsp.2011.08.001

[17] Zhou, Y., Wang, C., & Zhou, X. (2019). An Intra-Drift-Free Robust Watermarking Algorithm

in High Efficiency Video Coding Compressed Domain. *IEEE Access*, *7*, 132991–133007. https://doi.org/10.1109/access.2019.2940366

[18] He, Y., Yang, G., & Zhu, N. (2012). A real-time dual watermarking algorithm of H.264/AVC video stream for Video-on-Demand service. *Aeu-international Journal of Electronics and Communications*, *66*(4), 305–312. https://doi.org/10.1016/j.aeue.2011.08.007

[19] Su, P., Kuo, T., & Li, M. (2017). A practical design of digital watermarking for video streaming services. *Journal of Visual Communication and Image Representation*, *42*, 161–172. https://doi.org/10.1016/j.jvcir.2016.11.018

APPENDIX A
OUTCOMES

The expected outcome of this implementation is a notable reduction in piracy instances. The use of invisible watermarks adds an extra layer of protection, making it challenging for unauthorized users to detect and remove the embedded watermarks. Simultaneously, the visible watermarks serve as a clear indication of ownership, deterring any attempts at unauthorized recording or redistribution.

In the event that piracy does occur and a watermarked video is distributed without permission, the watermarks can be analysed to identify the user responsible for the unauthorized distribution. This outcome enhances the ability to take legal action against copyright infringement and hold individuals accountable for their actions.

In general, the project will successfully achieve the following outcomes:

- A software product based on 2 level watermarking to prevent piracy on OTT videos was implemented.
- Employed robust watermarks for each user and ensured that the employed watermarks are immune to external attacks.
- Preserved the visual quality of videos after watermarking.
- Minimized the processing complexity and resource consumption required for watermarking.
- A method to prevent piracy on OTT videos is to be implemented.

APPENDIX B
PROJECT TIMELINE

	Nov	Dec	Jan	Feb	Mar	Apr
Phase 1	■	■	■			
Phase 2			■	■		
Phase 3				■	■	■

Table B.1 Project Timeline

- **Phase 1:** Invisible Watermarking Module
- **Phase 2:** Development of OTT Platform and Visible Watermarking Module
- **Phase 3:** Implementation of the OTT Server and streaming setup

APPENDIX C
COST ESTIMATION

CATEGORY	COST
HARDWARE COSTS	
Laptop(Intel Core i5-1135G7 @ 2. 40GHz 1. 38 GHz,8GB RAM,512 SSD, Windows 10)	Rs. 65,550
Internet	Rs. 4,000
INDIRECT COSTS	
Indirect Costs	Rs. 5,000
TOTAL	**Rs. 74,550**

Table C.1 Cost Estimation

APPENDIX D

VISION, MISSION, PEOs & PSOs

D.1 Vision

To be a centre of excellence imparting quality education in Computer Science and Engineering and transforming students to critical thinkers and lifelong teams capable of developing environment friendly and economically feasible solutions to real world problems

D.2 Mission

- To provide a strong foundation in Computer Science and Engineering, prepare students for professional career and higher education, and inculcate research interest.
- To be abreast of the technological advances in a rapidly changing world.
- To impart skills to come up with socially acceptable solutions to real world problems, upholding ethical values.

D.3 Programme Educational Outcomes (PEOs)

PEO 1	Excel in professional career by acquiring knowledge in mathematics, science and, engineering and applying the knowledge in the design of hardware and software solutions for challenging problems of the society, adapting to the current tends by engaging in lifelong learning.
PEO 2	Pursue higher studies and research in the area of Computer Science and Engineering.
PEO 3	Ability to provide socially acceptable and economically feasible computer-oriented solutions to real world problems with teamwork, while maintaining environmental balance, quality and cognizance of the underlyingprinciples of ethics.

Table D.1 Programme Educational Outcomes

D.4 Programme Specific Outcomes (PSOs)

PSO 1	Apply mathematical and algorithmic principles, data structure concepts, software and hardware techniques in designing and developing optimized and secure computer-based solutions.
PSO 2	Design and develop system software and provide exposure to various tools and programming languages to facilitate efficient computing environment which adds to the case of human life.
PSO 3	Use the knowledge of various data processing, communication and intelligent systems to provide solutions to new ideas and innovations.

Table D.2 Programme Specific Outcomes

APPENDIX E

COURSE OUTCOMES

CO1	Model and solve real world problems by applying knowledge across domains (Cognitive knowledge level: **Apply**).
CO2	Develop products, processes or technologies for sustainable and socially relevant applications (Cognitive knowledge level: **Apply**).
CO3	Function effectively as an individual and as a leader in diverse teams and to comprehend and execute designated tasks (Cognitive knowledge level: **Apply**).
CO4	Plan and execute tasks utilizing available resources within timelines, following ethical and professional norms (Cognitive knowledge level: **Apply**).
CO5	Identify technology/research gaps and propose innovative/creative solutions (Cognitive knowledge level: **Analyse**).
CO6	Organize and communicate technical and scientific findings effectively in written and oral forms (Cognitive knowledge level: **Apply**).

Table E.1 Course Outcomes

APPENDIX F
PROGRAMME OUTCOMES (POs) ACHIEVED

Following are the various Programme Outcomes (POs) achieved through the implementation of the project.

PO1	**Engineering Knowledge**	Demonstrated an understanding of the fundamental principles of digital watermarking, including wavelet transformations, colour space conversion, and compression techniques. Explored how these techniques can be applied in the context of preventing piracy on OTT (Over-The-Top) platforms. Studied the algorithms and mathematical models underlying digital watermarking to ensure a solid grasp of the subject matter.
PO2	**Problem Analysis**	Identified the issue of piracy on OTT platforms as a significant problem affecting content creators and copyright holders. Conducted a thorough analysis of the various methods currently employed to prevent piracy and their limitations. Recognized the need for an innovative approach and proposed a new technique using watermarking as a potential solution. Analysed the strengths and weaknesses of watermarking in the context of preventing piracy.
PO3	**Design Development of Solutions**	Designed a comprehensive piracy prevention system that addresses the issue of piracy on OTT platforms. Developed an invisible watermarking model that embeds imperceptible watermarks into digital content, allowing for easy identification of pirated material. Additionally, designed a visible watermarking model that adds visible marks to discourage piracy. Integrated these models into a streaming setup, ensuring seamless integration with existing OTT platforms.

PO4	**Conduct Investigation of Complex Problem**	Conducted extensive investigations into the complex problem of piracy on OTT platforms. Conducted a literature review to gather existing research and insights related to watermarking techniques. Experimented with different algorithms and methodologies to validate the proposed solution. Conducted performance evaluations and comparative analyses to assess the effectiveness of the watermarking-based piracy prevention system.
PO5	**Modern Tool Usage**	Leveraged various modern tools and techniques to design and implement the piracy prevention system. Utilized the FFmpeg tool for efficient video processing and manipulation. Developed mobile applications using Android Studio and Flutter to demonstrate the integration of the watermarking system with OTT platforms on mobile devices. Employed Flask framework to create a web-based interface for system administration and monitoring.
PO6	**The Engineer and Society**	Recognized the far-reaching impact of piracy on the digital economy and society as a whole. Acknowledged the importance of protecting the rights of content creators and ensuring fair compensation for their work. Proposed a solution that benefits both content creators, by deterring piracy, and consumers, by promoting access to legitimate content through OTT platforms.
PO7	**Environment and Sustainability**	Considered the environmental impact of the piracy prevention system and proposed a streaming setup that minimizes buffering and energy consumption. Optimized the system architecture to ensure efficient resource utilization. Balanced the need for robust piracy prevention with environmentally conscious practices.
PO8	**Ethics**	Considered the ethical implications of the piracy prevention system throughout the project. Upheld the principle of fairness by protecting the intellectual property rights of

		content creators. Ensured that the watermarking system respects user privacy and does not infringe upon their rights. Strived to create a system that encourages creativity and rewards original content.
PO9	**Individual and Team Work**	Demonstrated both individual and collaborative work throughout the project. Took responsibility for personal tasks and delivered on deadlines. Actively sought and incorporated feedback from supervisors and peers. Collaborated with team members to integrate different components of the piracy prevention system and ensure seamless functionality.
PO10	**Communication**	Effectively communicated ideas and findings throughout the project. Presented research findings, system designs, and experimental results in a clear and concise manner. Engaged in regular meetings with the project team and supervisors to provide updates on progress and address any concerns or questions. Prepared documentation and reports to facilitate knowledge sharing and future reference.
PO11	**Project Management and Finance**	Effectively managed the project within the allocated time constraints. Developed a project plan outlining tasks, timelines, and resource requirements. Monitored progress and made necessary adjustments to ensure project milestones were met. Demonstrated financial acumen by considering budgetary constraints and optimizing resource allocation.
PO12	**Life-Long Learning**	Demonstrated a commitment to lifelong learning by acquiring new knowledge and skills in the area of digital watermarking. Stayed updated with the latest research and advancements in the field.

Table F.1 Programme Outcomes Achieved