Proceedings of the Second International Conference on Automation, Computing and Renewable Systems (ICACRS-2023)
IEEE Xplore Part Number: CFP23CB5-ART; ISBN: 979-8-3503-4023-5

2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS) | 979-8-3503-4023-5/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICACRS58579.2023.10404733

Forensic Video Watermarking

Elavarasan S.R [2]
Department of networking and communications
Srm Institute of science and technology
Kattankulathur,India
es9964@srmist.edu.in

DR.S. Metilda Florence[1]
Department of networking and communications
Srm Institute of science and technology
Kattankulathur, India
metildam@srmist.edu.in

***Abstract* — The aim of forensic watermarking is to trace out unauthorized users who are responsible for distribution of illicit digital content. Although there are many approaches for preventing of pirated video in the internet such as video watermarking the content but the real time implementation of the watermarked video and distributing in the streaming platforms is complex and also expensive. In this paper we are going to propose a solution by implementation of a low-cost server-side blind watermarking using a/b watermarking. Although there are traditional watermarking methods for distributing the video, we discussed about the real time watermark generation and embedding and distributing to the users during live streaming. Here we will be dividing live video stream content as A and B to the nginx server the nginx server embed the watermark using a script and store it as an input. When a user requests the live video the node.js script sequence a particular watermark content to the user so that for every frame sequence each user gets a different type of video. If suppose when the live video is pirated when can find the user by the sequence of the watermark which is sent to the user.**

Keywords— Server-side watermarking, Nginx server, RTMP, Live video, Low cost.

I. INTRODUCTION

Forensic watermarking is a method which is used to embed the information in an image, video or a text to protect the ownership or copyright of the information. A digital watermark is a type of identifier that is anonymously inserted into an image, video, or audio stream that can withstand any external artifacts. The watermark is used to identify and protect the owner and also ensure the assurance and the integrity of the individual and also used to track copyright violations. There are several types of video watermarking in streaming platforms but still the media, OTT platforms face the difficulties of pirated video which is leaked and spreaded over the internet by unauthorized users. Though there are several traditional methods of watermarking methods in video for protecting ownership, it has some complications such as visible watermarking and also expensive to implement this method in real time. This paper represents a low-cost implementation of a/b watermarking over traditional methods of watermarking which introduces a term called as invisible watermarking. In this method we are using a live streaming video using rtmp protocol using nginx server. The live stream video is converted to chunks for reducing the size of the video. Here we are creating two types of directories A and B for storing the video information after the video a separated into chunks a small automated python script runs at the backend of the server which creates and separate the video chunks into two video directories A and B and for invisible watermark embedding in the live video. Here the invisible watermark is embedded in two directories A and B. After embedding and storing it in a server. If a user requests the live video a small node.js UUID script is run at backend of the server which is responsible for sequencing the live video in a mix of sequence to each and every user so that if a user tries to pirate a video by finding the sequence of the chunks of the video and the invisible watermark, we can find the unauthorized user and block their access. This method can be implemented in small scale live streaming applications with minimal cost.

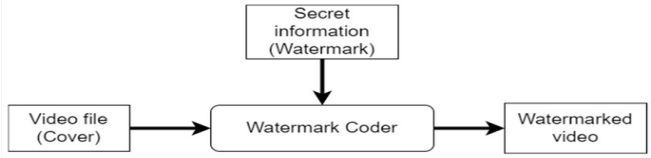

Fig.1 Forensic Video Watermarking

II. LITERATURE SURVEY

There are various types of watermarks embedding and packaging methods which was discussed earlier. In Marren H et .al,[1] it discusses about concepts of implementing the robustness of the video using the method for preserving the a/b watermarking method with high scability. However high video quality content with bitrate of very low content are some key aspects for a good working of watermarking technique with the existing solutions. In some studies, they discussed about a solution for distributing videos in large scale distribution which is inspired by a/b watermarking technique. Improvement in watermark embedding at low complexity and faster watermark detection method, which act a baseline for the a/b watermarking technique but it is applied only at the frame level still improvements have to be done when it comes to application in segmentation of video [4]. They also gave an idea about how to give an approach for watermark embedding which achieve the quality of the video and compress the artifacts. And also, this method ensures the anyone can perform the detection of watermarked content without losing the robustness of the video [5]. In Yu X et al, Analysis about the algorithms which have been used for detection of illegal pirated video content, what is the algorithm behind it different types of watermarking methods and also, they have given a report and differentiation about the how the watermark content can be detected what are the types and the methods are used here and a summarization of all the methods were discussed for future research [2]. In Su

Pc et al, an approach for implementing the forensic watermarking method for digital content has been done. They have designed in such a way that they can embed the watermark at the frames of the video so that the server can sequence the video in much faster manner and also it adds the feature that when the video is pirated still then by using the signal which has been hidden inside the frames can be detected without affecting the originality of the video content but further some small changes required for video encoding and decoding process.[3]

III. OVERVIEW

Researchers have proposed some of the existing method for the implementation of real time digital watermarking methods but there are some drawbacks when it comes to live stream real time implementation which includes traditional visible watermarking.

Traditional watermarking: Large-scale media and over-the-top platforms applications heavily rely on standard video content with visible watermarking. By safeguarding intellectual property and advancing the brand, it performs the functions of two tools in one. For the purposes of quality assurance, user attribution, content monitoring, and legal protection, watermarks are necessary. When used properly, they enhance the viewing experience and user engagement, which eventually helps platforms that disseminate content as well as content providers. As a security precaution, watermarking is not impervious to assaults. The authenticity of research data is at risk because determined adversaries may try to erase or modify the watermark. Conventional digital watermarks could not provide sufficient security in situations when the legitimacy of the study is crucial. Using content that is protected by copyright is common in research. For research purposes, adding digital watermarks on such content might cause ethical and legal issues. When using classic watermarked techniques in their work, researchers have to deal with these complex issues.

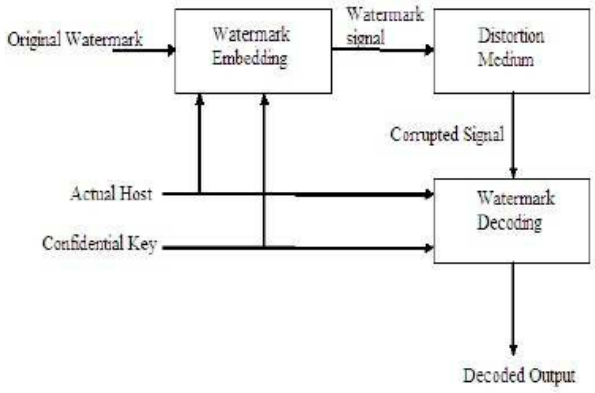

Fig 2. Traditional watermarking

This method ensures the confidentiality and protect against unauthorized copying, distribution, and piracy. This helps content creators and distributors safeguard their intellectual property rights.

IV. PROPOSED METHODOLOGY

In this method an implementation of a/b watermarking is done in terms of low cost, reduced complexity in watermark embedding and increase the robustness of the live video during the streaming of the video which consist the invisible watermark information .For this we are going to work with the virtual server instance which is offered by oracle which has enhanced and allocated the instance to boost up the performance of the video encoding process when compared to other cloud service providers, For implementation here we will be using ubuntu which is a type of Linux distro ,the user can connect to the instances using third party client software, for this here we will be using PuTTY software for connecting the instance to the server using SSH protocol. For reducing the complexity during watermark embedding process there are so many transformation methods which has been proposed earlier but there is complexion while transformation of image and embedding the watermarking in between the frames of video in order to overcome the complexity a small automated python script which runs at the backend of the server so that during live streaming the watermark automatically embeds into the digital live streaming.

V. PROPOSED ARCHITECTURE

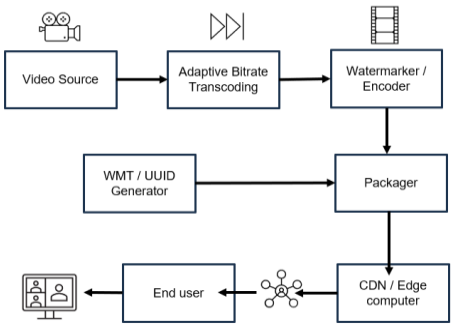

Fig.3. Proposed Architecture

- This method proposes about the functional architecture about the implementation of a/b watermarking. the source of the vvideo feed is received as RTSP and RTMP stream if the source is live, for the on-demand video content ffmpeg is used to stream the offline video as RTSP or RTMP. For Adaptive Bitrate Transcoding, RTMP Media Streaming Module is used for the transcoding the feed into segments or chunks. For Watermarker Encoder, Ffmpeg is used to add watermarks to video segments and several options you can use to place them in different positions in a video. For video packaging Bento4 MP4HLS mp4dcfpackager all the segments are packed into the HLS manifest file along with the watermark id from the watermark token generator. For Watermark token Each and individual user session will get a unique user identification token from the node.js UUID module.

VI. RESULTS

The video watermarking for the live video source is done with Arm-based compute from Oracle Cloud adaptable virtual machine ranges from 1 to 80 cores and 1 to 64 GB of RAM per core [6]. The live video source is associated with the rtmp

protocol and using the video transcoding i.e ABR (adaptive bitrate) conversion happens which divides the raw video source content into small segments or chunks and that hit is streamed using this virtual machine instance.

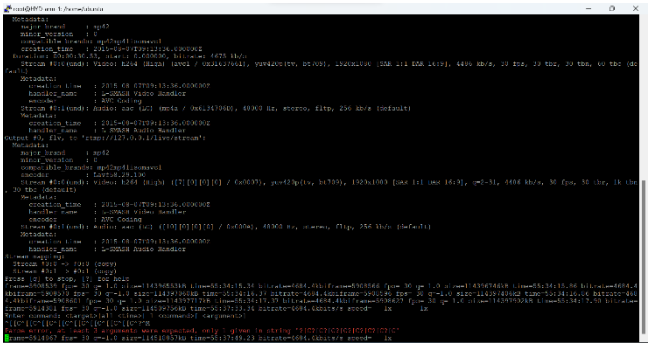

Fig.4. Output of video encoding

When the live stream happens parallelly, the video encoding happens, the ffmpeg tool which act as an input to the watermark embedder into the live stream video segments, furthermore during transcoding process this ABR is divided into two variants A and B, two different types of invisible watermark is embedded into two variants in each segment level, the input script in ffmpeg tool is automated so that whenever the user request the live video it embeds the invisible watermark into the live video stream and it stores it in the server before they are been delivered to the packaging and the sequencing of these variants should happen in the live stream so that when the user request the live video it generates the UUID token along with the unique watermark identifier. It reduces the time complexity of the architecture when it comes to real time implementation.

VII. CONCLUSION

In this project, an architecture was proposed for the forensic digital video watermarking which overcomes the time complexity and implementation cost for the real time live streaming in OTT and streaming platforms. Additionally, the implementation of live video watermarking in the server-side without the loss of robustness was the challenging part in this project and also it enhances the masking method of identifying the real user session ID in the node.js script which easily finds out the unauthorized user who is responsible for pirating the video.

VIII. FUTURE SCOPE

In future, there will be an enhancement in detection of the unauthorized user who is responsible for pirating the video during the live stream.

IX. REFERENCES

1. Mareen H, Van Wallendael G, Lambert P. Implementation-free forensic watermarking for adaptive streaming with A/B watermarking. InProceedings of Sixth International Congress on Information and Communication Technology: ICICT 2021, London, Volume 1 2022 (pp. 325-339). Springer Singapore.

2. Yu X, Wang C, Zhou X. A survey on robust video watermarking algorithms for copyright protection. Applied Sciences. 2018 Oct 11;8(10):1891

3. Mareen H, Courteaux M, De Praeter J, Asikuzzaman M, Van Wallendael G, Lambert P. Rate-distortion-preserving forensic watermarking using quantization parameter variation. IEEE Access. 2020 Mar 30;8:63700-9.

4. Su PC, Kuo TY, Li MH. A practical design of digital watermarking for video streaming services. Journal of Visual Communication and Image Representation. 2017 Jan 1;42:161-72.

5. Mareen H, Valcke F, Hallaert A, Van Wallendael G, Lambert P. Watermarking for Large-Scale Video Distribution through Out-of-the-Loop Frame Replacement. In2022 10th European Workshop on Visual Information Processing (EUVIP) 2022 Sep 11 (pp. 1-6). IEEE.

6. https://www.oracle.com/in/cloud/compute/arm/

7. https://en.wikipedia.org/wiki/Digital_watermarking

8. https://reports.valuates.com/market-reports/QYRE-Auto-14E15487/global-forensic-video-watermarking-solution

9. https://massive.io/content-security/what-is-forensic-watermarking/

10. https://www.geeksforgeeks.org/digital-watermarking-and-its-types/-lifecycle