Tracking of Video Piracy using Unique Identifier

Dr. Sheeja Agustin[1], Aleena Nair[2], Aravind Ajit[3], Aravind R[4], Jayanth Indalvai Reddy[5]

[1]Associate Professor, Department of Computer Science & Engineering, Marian Engineering College APJ Kerala Technological University, India

[2,3,4,5]B.Tech Student, Department of Computer Science & Engineering, Marian Engineering College APJ Kerala Technological University, India

***Abstract* - Any video that is uploaded on a streaming platform is encrypted with a UID that is specific to the account holder. When user downloads a video his UID is hidden within the video. If the user uploads his downloaded video on a third party site, they can be tracked by using the hidden UID. This unique identification contains the information about the user. Video steganography is implemented as the main method.**

***General Terms* - Information Hiding, Image, Video, Quality, Security**

***Index Terms* – Steganography, Caesar Cypher.**

I.INTRODUCTION

As streaming platforms, and the digital availability of entertainment content are both rapidly increasing, the demand for the instant scope of the latest movies or TV show is becoming a norm.

Even though registered content distributors such as VOD platforms are also increasing in growth, thus giving instant access to entertainment content, video piracy seems more popular than ever because not all content can be accessed legally at the same time in every market; therefore the search through mostly non user-friendly content libraries of countless providers becomes a taxing and nerve-wracking task, and it is not without cost. In addition, unlike a few years ago, the available pirated content for download and streaming options are high quality.

Thus, video piracy is a easier, more convenient, cost-free, and even socially acceptable choice.

However, it is also not a secret anymore that the distribution of copyrighted material is illegal, nor that it causes financial dip to rights holders. Furthermore, everyone should know the vast consequences of video piracy by now. The risk of being able to overcome the costs of film production has increased in recent years, which has led to a thinning of independent and smaller producers and the rise of already established filmmakers and studios.

The media and entertainment industry will gradually lose its versatility.

Modern video content owners have an number of ways they can try to protect their movies or general media content from pirated online distribution; the possibilities range from watermarking videos also a possible aspect of new release strategies to sending warnings and closing down piracy sites.

Aside from the fact that many content protection options are extremely expensive and therefore only accessible to large rights holders, piracy advocates mock it as a bottomless pit when trying to block streaming video piracy.

As soon as some piracy sites or streaming channels close, multiple new ones are created.

II.STEGANOGRAPHY

A. Steganography [5]

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted at its destination. The use of steganography can be coupled with encryption as an extra step for hiding data.

It can be used to disguise almost any type of digital content, including text, image, video or audio content basically all types of multimedia’s; the data to be hidden can be concealed inside almost any other type of digital content. The content to be hidden through steganography -- called hidden text -- is more often than not encrypted before being integrated into the innocuous-seeming cover text file or data stream. If not encrypted, the concealed text is commonly processed in some way in order to up the difficulty of detecting the secret content. It is practiced by those wanting to convey a secret message or code. While there are many legal uses for steganography, malware developers have also been found to use steganography to their advantage, to obscure the transfer of malicious code.

Different forms of steganography have been used for centuries and comprise almost any technique for hiding a secret message in an otherwise safe container. For example, using invisible ink to conceal messages in otherwise harmless messages; hiding documents recorded on microdot -- these can be as small as 1 millimeter in diameter -- inside legitimate-seeming correspondence; and even by using multiplayer gaming simulations to share information.

B. Steganography Techniques

In modern digital steganography, data in the first stage is encrypted or obfuscated in some other method and then inserted, using a particular algorithm, into data that is part of a special file format such as a JPEG image, audio or video file. The secret message can be inserted into ordinary data files in a variety of different ways. One technique is to conceal data in bits that represent the same

colour pixels recur in a row in an image file. By putting in the encrypted data to this redundant data in some subtle way, the output will be an image file that appears similar to the original image but that has patterns called the “noise” patterns of regular, unencrypted data.

The implementation of adding a watermark -- a trademark or other identifying data concealed in multimedia or other content files -- is one usual use of steganography.

Watermarking is a method often used by online publishers to detect the source of media files that have been found being transmitted without permission.

While there are a variety of uses of steganography, including embedding sensitive information into file types, one of the most applied techniques is to embed a text file into an image file. When this is done, anyone accessing the image file should not in any way be able to see a difference between the original image file and the encrypted file; this is achieved by storing the input message with less significant bites in the data file. This whole technique can be concluded manually or with the use of a steganography tool.

C. Steganography Software

Steganography software is used to carry out a variety of functions in order to hide data, including encoding the data to prepare it to be hidden inside another file, keeping track of which bits of the cover text file contains concealed data, encrypting the data to be hidden and extracting hidden data by its authorised recipient.

III. STEGANOGRAPHY USING PYTHON

Encode the data :

Every byte of data is transformed to its 8-bit binary code using ASCII values. These pixels are read from left to right in a group of 3 containing a total of 9 values. The initial 8- values are used to store the binary data. This value is then made odd if 1 occurs and even if 0 occurs. [4]

Decode the data :

During the decode phase, three pixels are read at a time, till the end value is odd, which means the message is completed. Every 3-pixels contain binary data, which can be obtained by the same encoding logic. If the value is found to be odd the binary bit is 1 else 0.

IV. CAESAR CYPHER

The Caesar Cypher technique is one of few of the earliest and easiest methods of encryption technique. It’s basically a type of substitution cypher, where each letter of a text is written over by a letter by some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The technique is apparently named after Julius Caesar, who used it to communicate with his immediate officials. Thus to cipher a given text we would need an integer value, known as a shift which tells us the number of position each letter of the text has been moved down. The encryption can be brought about by using modular arithmetic by first transforming the letters into numbers, according to the method, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be related mathematically as. [3]

$$E_n(x) = (x + n) mod\ 26$$

(Encryption Phase with shift n)

$$D_n(x) = (x - n) mod\ 26$$

(Decryption Phase with shift n)

V.METHOD

Video steganography is applied as the main method. Any video that is uploaded on a streaming platform is encrypted with a UID that is specific to the account holder. When a user downloads a video his UID is hidden within the video. If the user uploads his downloaded video on a third party site, they can be tracked by using the hidden UID. This unique identification contains information about the user.

There are two phases, the first phase is the encryption that happens when the video is created. For every user, a unique identifier (UID) is created and is hidden in the video. The way that is done is by hiding the UID in every 60th frame of the video using an algorithm. When the said video is downloaded the UID is hidden within it.

In the second phase the process of decryption occurs. If the downloaded video is uploaded to a third-party site the video is downloaded by us to decrypt the hidden UID. These third- party sites are continuously monitored for new uploads by us. Using this decrypted UID we can track the users account details thus identifying the source of the piracy.

VI.EXPERIMENTAL DESIGN

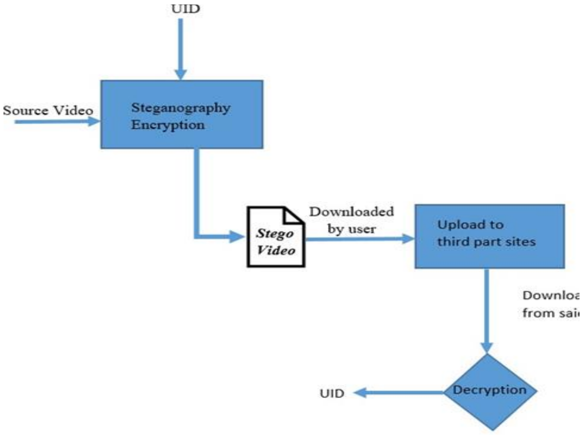

Fig 1: Video piracy detection.

A. Encryption and Merging text into video

- Input the location of video file
- Input the Caesar Cypher value
- If the file is not found error message is displayed “File is not Found” in command prompt.
- Extract the frames from video

1. Make a temp folder
2. Remove the temp folder if exists
3. Get the batch of the video frames using openCV
4. Loop through the batch of frames and write each frame in said above temp folder
5. Repeat the step until the last frame

- Extract audio from video using ffmpeg
- Encode the frame

1. Read text file which we are using to hide
2. Loop through the text file until last frame and encrypt and encode each text to the frames

- Merge the frames using ffmpeg
- Merge the audio using ffmpeg

VII.MODULES

Module 1. Embedding process

This process is carried out at the senders side where secret message is embedded inside each frame of the video using ffmpeg

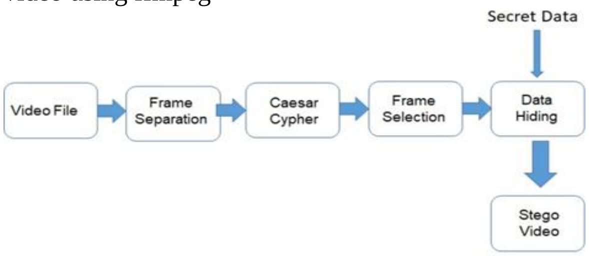

Fig 1. Embedding

Module 2. Extracting Process

Reverse of the embedding process where the data is collected and decrypted using the Caesar cypher.

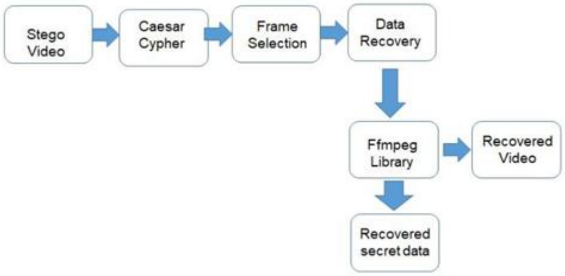

Fig 2. Extraction

VIII.CONCLUSION

Reducing piracy in a way that does not subject further findings of pirated copies. Encrypting individual frames with the encrypted unique identifiers helps remove any media online that is not authorised. Security protection in steganography is very high from cryptography and it is very useful to explore stego videos to avoid cybercrimes and for breaking the planning strategies of terrorists.

IX. ACKNOWLEDGEMENT

The authors would like to thanks to the earlier work regarding different video piracy tracking that contribute the work made in this paper. All work done in this paper will help to the researchers for doing future work based on video steganography.

REFERENCES

[1] RAMANDEEP KAUR, POOJA, VARSHA, “THE NON- TANGIBLE MASKING OF CONFIDENTIAL INFORMATION USING VIDEO STEGANOGRAPHY”, INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS (0975 – 8887) VOLUME 119 – NO.17, JUNE 2015.

[2] E. ANNA DEVI, R. M. JOANY, S. YOGALAKSHMI, L. MAGTHELIN THERASE4, “DIGITAL VIDEO STEGANOGRAPHY TECHNOLOGY FOR SECURITY APPLICATION”, INTERNATIONAL CONFERENCE ON FRONTIERS IN MATERIALS AND SMART SYSTEM TECHNOLOGIES IOP CONF. SERIES: MATERIALS SCIENCE AND ENGINEERING 590 (2019).

[3] https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

[4] https://www.geeksforgeeks.org/image-based-steganography-using-python/

[5] https://searchsecurity.techtarget.com/definition/steg anography