Video Piracy Detection using Invisible Watermark

Anjali Tiwari[1], Harsh Shah[2], Unnati Thube[3], Nasim Shah[4]
[1-3]BE Student, Information Technology Department [4]Faculty of Information Technology Department
K.J. Somaiya Institute of Engineering and Information Technology, Mumbai, India

***Abstract:*- Piracy is an important issue as far as the manufacturers are concerned as it can result in a huge revenue loss. The aim of our project is to detect video piracy using invisible watermark, i.e. Invisible Digital Watermarking is a technique of steganography. Invisible Digital Watermarking is a technique of steganography to manipulate frames of the video by modifying the pixels scattered across the frame. The bits are modified with reference to original RGB value and a slight modification is imposed on basis of the KEY used while watermarking. The slight shift in RGB value scattered across makes it impossible to visibly detect the difference when compared to original video.**

Keywords—Steganography, Digital watermark.

I. INTRODUCTION:

Invisible digital watermarks are a new technology which could solve the “problem” of enforcing the copyright of content transmitted across shared networks [9].Copyright protection has been a problem since the advent of compact discs. Several methods have been implemented for preventing the copyright information from being muddled with, like stenographic algorithms, cryptographic techniques and the new era technology watermarking. The goal of this project is to use digital watermarking techniques to detect video piracy. A digital watermark is a distinguishing piece of information that is adhered to the data that it is intended to protect, this meaning that it should be very difficult to extract or remove the watermark from the watermarked object. The information watermarked may include owner, recipient and/or distributor details, transaction dates, serial numbers, etc. which play an important role in determining which of the copies, have been pirated.

II. DRAWBACKS OF EXISTING SYSTEM:

Digital Watermarking is an adaptation of the commonly used and well-known paper watermarks to the digital world. Digital watermarking describes methods and technologies that allow hiding information, for example a number of texts, in digital media, such as images, video and audio. As the watermark is visible to the users, they can easily manipulate those portions of the image alone. The watermark though efficient is concentrated in a particular area, thus through statistical analysis the approximate location of the watermark can be identified. This enables the hackers to overwrite the copyright information with their own information.Another method present which is piracy detection of movies using forensic watermarking.[7]. the goal of the watermark is to help to identify the source of an unauthorized copy of media files and retrace them back to the copyright authorized recipient or legitimate content holder. The presence of or identifying the watermark will arise the copyright infringement over the third party. And to deter piracy in the content distribution the user is a media-aware-before-hand-that the content is made traceable to the last authorized recipient.Drawback of this system is very costly.

III. PROPOSED METHODOLOGY

A digital watermark is a marker that gets embedded within a image such as Video, audio or image data. Digital Watermarking is the process of hiding digital information in image.Digital watermarks are prominently used to verify the authenticity or integrity of the carrier signal and also to deduce the identity of its owners. It is prominently used for tracing copyright infringements.

Cryptography:

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography the only means of providing information security.[8]

Steganography

Steganography is the science of hiding information. Whereas the goal of cryptography is to make data unreadable by a third party, the goal of steganography is to hide the data from a third party. Hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message There are three main ways to conceal the secret message/image. The first way is straight insertion where you just put the message into the cover image. The next way requires some analysis to find the variations in color and it puts the message in those areas where it is less likely to be detected. The last way is to randomly insert the message into the image.

Digital watermarking

Watermarking is sub-discipline of information hiding.Digital watermarking is a technology for embedding various types of information in digital content in general, information for protecting copyrights and proving the validity of data is embedded as a watermark.[8] Digital watermarks apply a similar method to digital content. Watermarked content can prove its origin, thereby protecting copyright. A watermark also discourages piracy by silently and psychologically deterring criminals from making illegal copies. A digital watermark is a distinguishing piece of information that is adhered to the data that it is intended to protect, this meaning that it should be very difficult to extract or remove the watermark from the watermarked object.

IV. METHODOLOGY

Video Header Information

The video information is stored in AVI RIFF format. The various headers and chunks are identified and declared. Thus by identifying the header information the location of the data is found.

File Handling Module

The information about the owner, recipient/distributor, serial number and other copyright related data is stored in a text file. This Write the byte to result text file Stop information is read from the text file. The information in the video file is also read and two new files the key file and a temporary file are created. The header information is read from the video file and is written into the key file and the temporary file. The file- handling module is carried out both during watermarking and detection of watermarking.

Watermarking Module

The image is watermarked with the copyright information such a way that the video information does not lose its property. Changing a few data bits of the video file depending on the copyright information does this. The key file generated in this process should be kept secret and should be protected from any corruption.

Detection Module

The data from the watermarked video file is fetched during check for piracy. Using the key file the copyright information is extracted from the watermarked data. From the copyright information it is possible to find the source of piracy and thus necessary action can be taken.

Integration and Security

Errors in each of the modules are handled separately. Once this is done, the various modules are integrated and the errors that follow are handled.

V. ALGORITHM

Watermarking Process:

1. A Video which to be watermarked is taken as an input.
2. Divide the video into frames using Matlab.
3. Importing bits from frames using Java.
4. In the video, locations should be selected where the text file needs to be embedded.
5. a) Assigning the codes to respective locations.
   b) Making a key file of the location of the embedded text files.
6. The frames should be integrated as a video again.
7. The video now obtained will be a watermarked video.

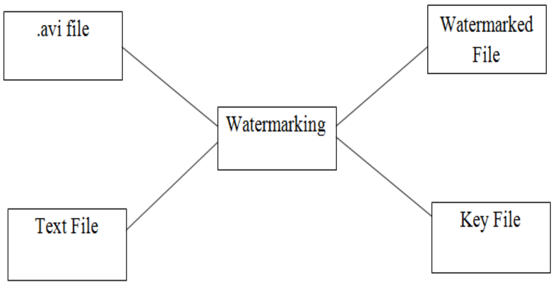

Fig:1 Block diagram of Watermarking

Detection of Piracy:

1. Video to be tested is taken as a video.
2. Divide the video into frames using Matlab.
3. The key file is compared with the key file generated from the video using Java.
4. a) If true, Video is not pirated
   b) If false, video is pirated.

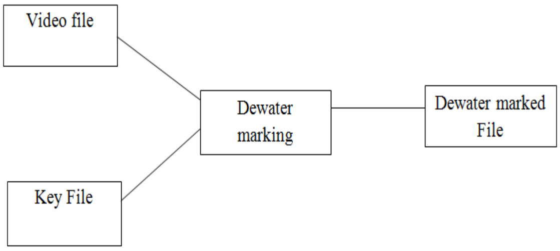

Fig:2 Detection of watermarking

VI. CONCLUSION

Compared to some of the other recent techniques our proposed system turns out to be in terms of difficulty in modifying the video content which is invisibly watermarked by using Stegonagraphy . The detection of video piracy is relatively easier , simpler and secure due to the password protected key which is available only to the owner of the video.

VII. REFERENCES:

1. International Social Science Conference (ISSC),2013 Robust Digital Video Watermarking using Reversible Data Hiding and Visual Cryptography.
2. International journal of Computer Applications, Feb 2013 Anti-Piracy For Movies using Forensic Watermarking.
3. International Journal of Emerging Science and Engineering (IJESE) , September 2013 Watermarking On Compressed & Encrypted JPEG 2000 Images Using Rational Dither Modulation
4. International journal of Computer Application & Information technology, Sept 2012 Classification of Watermarking Based upon Various parameters.
5. IEEE, June 2012 Robust watermarking of compressed and Encrypted JPEG2000 Images.
6. International Journal of Advanced Research in Electronics and Communication Engineering ,2012 Hardware implementation of Digital Watermarking System for Video Authentication.
7. Video Content Recognition Systems Attrasoft White Paper, Jan 2008 Attrasoft Fingerprint.Detect.Measure.
8. Indian journal of Computer Science and Engineering Digital Watermarking Schemes For Authorization Against Coping or Color Images
9. International journal of Computer Applications, August 2010 Invisible Digital Watermarking Through Encryption.