RESEARCH ARTICLE OPEN ACCESS

Invisible Watermarking: New Approach for Video Piracy Detection

Manisha Bhagat[1], Komal Chavan[2] ,Shriniwas Deshmukh[3]
[1,2,3](Computer Department, Modern Education Society's College of Engineering, and Pune,)

Abstract:

Today piracy is one of the most important issues that the owners of multimedia contents are facing now. So it becomes necessary to protect the copyright of digital media. The new technology proposed to solve the "problem" of enforcing the copyright of content transmitted across shared networks is Invisible Digital Watermark. It is a technique of steganography that allow a copyright holder to insert a hidden message (invisible watermark) within images, sound files, moving pictures and even raw text. To watermark a video it is divided into frames then extract each bit of a frame and modify it with reference to original RGB value to embed a watermark in it. The location of the embedded text is maintained as a key file and the frames are integrated as a video again. The slight changes in RGB value scattered across the frame makes it impossible to visibly detect the difference when compared to original video. To detect the piracy of video 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.

Keywords — **hacking, authentication, cryptography, steganography, copyright.**

I. INTRODUCTION

With the advancement in technology the distribution of video data is much easier and faster. Since digital video sequences can be easily manipulated, concerns regarding authentication of the digital video are increasing. In situations where the video data should be credible, that is when it needs to be used as evidence, this issue becomes serious. So we need authentication techniques to maintain authenticity, integrity, and security of digital video content. Invisible digital watermarking is one of the key authentication methods. Digital watermarking is the process of embedding additional, identifying information within a host multimedia object like a video. By adding a transparent watermark to the multimedia content, we can verify the ownership of the digital media and detect video piracy. A digital watermark is a distinguishing piece of information that is embedded in 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.

Digital Watermarking is similar to the commonly used paper watermarks to the digital world .Digital watermarking describes methods and technologies that allow hiding information in digital media, such as video. As the watermark is visible to the users, they can easily change those parts of the image alone .Though the watermark is efficient concentrated in a particular area, thus through statistical analysis the approximate location of the watermark can be identified. This helps the hackers to overwrite the copyright information with their own information. Another method present which is piracy detection of movies using forensic watermarking .The goal of the watermark is to help to identify the source of an unauthorized copy of media files and again trace them back to the copyright authorized recipient. Drawback of this system is very costly.

III. PROPOSED SYSTEM

A digital watermark is a pattern of bits inserted into a digital file -image, audio or video. Such messages usually carry copyright information of the file .Digital watermarking takes its name from

watermarking of paper or money. But the main difference between them is that digital watermarks are supposed to be invisible or at least not changing the perception of original file, unlike paper watermarks, which are supposed to be somewhat visible. Embedding a watermark should not result in a significant increase or reduction in the original data.

Cryptography:

Cryptography is the science of analyzing and deciphering codes and ciphers and cryptograms. It helps in information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

Steganography:

Steganography is the study of hiding information in such a way that others cannot feel the presence of contents of the hidden message. There are three main ways to hide the secret message. The first way is direct 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 in a simple way is hiding information .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. 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 stopping criminals from making illegal copies. A digital watermark is a unique piece of information that is attached or embedded with the data that it is intended to protect.

IV. IMPLEMENTATION MODULES

A. Header Information Of The Video:

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

B. File Handling Module:

The information about the owner, distributor, serial number and other copyright related data is stored in a 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.

C. *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.

D. 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.

E. Integration And Security:

Errors in each of the modules are handled separately and then the modules are integrated and the errors that follow are handled.

IV. ALGORITHM.

For watermarking:

1. Take video file as input.
2. Use Matlab to divide video into frames.
3. Using java import bits from frames.
4. Select Location to insert information.
5. Assign code for selected location.

6. Create key file to store location information.
7. Convert frames into video.

For Piracy Detection:

1. Take testing video as input.
2. With Matlab divide it into frames.
3. With java compare actual key file with generated key file.
4. True-video not pirated.
   False-video pirated.

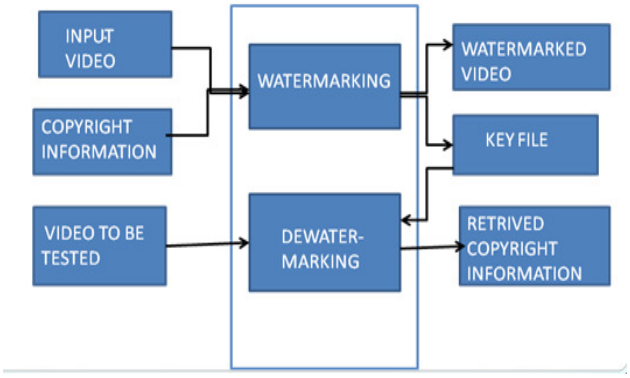

Fig 1. Block Diagram

Encoding process:

This system performs Encode process. User selects input video file (i.e. Source video), from where information of video is collected. User also provides output video file where encoded video is going to be stored with message to be hidden. For encoding purpose LSB Replacement / Substitution Technique is used.

When the video files are created, there are usually some bytes in file that are not needed /important. These areas of file can be replace with information i.e. to be hidden without damaging it. This method is called as LSB replacement Method and generally used for Image and video files. The value 11111111 can be replaced by 11111110 which is unpredictable by Human Eye.

Example:

Video are made up of frames and frames consist of thousands of pixels. Each pixel is made up of RGB (Red, Green and Blue) color. Each color of RGB is represented by 8-bits of data.

	R	G	B
1st Pixel	(00100111	11101001	11001000)
2nd Pixel	(00100111	11001000	11101001)
3rd Pixel	(11001000	00100111	11101001)

So we use three pixel to store one byte of message.
Suppose we want to store/encode character A.
Let Character A=10000001, is inserted, the following result occurs-

	R	G	B
1st Pixel	(00100111	11101000	11001000)
2nd Pixel	(00100110	11001000	11101000)
3rd Pixel	(11001000	00100111	11101001)

So resulting pixel of video have slightly changed values which is undetectable by Human Eye.

Decoding process:

Decoding process is exactly opposite to encoding. Here we simply reads only LSB (least significant bit) and combine these bit into bytes where each byte will represent a character. These characters in turn form a message. In this way original message is retrieved.

Example:

As we already encoded message into video. We will consider encoded pixel of above example,

	R	G	B
1st Pixel	(00100111	11101000	11001000)
2nd Pixel	(00100110	11001000	11101000)
3rd Pixel	(11001000	00100111	11101001)

This produces bit sequence 10000001, where 10000001 presents A. So message retrieved is A.

VI. CONCLUSION

Though there are various methods available for protecting the copyright and similar issues, digital watermark is used because of its advantages like being robust, fragile and imperceptible nature.

The proposed system in this project has used invisible digital watermarking technique to detect video piracy and has overcome most of the major shortcomings of the existing system .It has several advantages as compared to existing systems.
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. ACKNOWLEDGMENT

We would like to take this opportunity to thank our internal guide Prof. D.D. Ahir, for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.

We are also grateful to Dr. N. F. Shaikh, Head of Computer Engineering Department, M E S College of Engineering for her indispensable support, suggestions.

In the end our special thanks to the college for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

VIII. REFERENCES

1. Samir Kumar Bandyopadhyay, TuhinUtsab Paul, AvishekRaychoudhury"Invisible Digital Watermarking Through Encryption", International Journal of Computer Applications (0975 – 8887), Volume 4– No.8,August 2010..

2. Jayamalar T, Radha V (2010) "Survey on Digital Video Watermarking Techniques and attacks on Watermarks", International Journal of Engineering and Technology, Vol. 2(12), Pp 6963-6967, 2010.

3. Karnpriya Vyas ,Kirti Sethiya and Sonu Jain, (2012), 'Implementation of Digital Watermarking Using MATLAB Software' , AN INTERNATIONAL JOURNAL OF ADVANCED COMPUTER TECHNOLOGY, 1 (1), Volume-I, Issue-I (2012).

4. Wiktor Starzyk, Faisal Z. Qureshi, Multi-tasking Smart Cameras for Intelligent Video Surveillance Systems at 8th IEEE International Conference, 2011.

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. Ling Na Hu Ling Ge Jiang, "Blind Detection of LSB Watermarking at Low Embedding Rate in Grayscale Images," In: M. Celik, G. Sharma, E. Saber and A. Tekalp, Eds., Hierarchical Watermarking for secure Image Authentication with Localization, IEEE Transactions on Image Process, Vol. 11, No. 6, 2002, pp.
585-595, June 2002.

9. L. Chih-Chin and T. Cheng-Chih, "Digital image watermarking using discrete wavelet transform and singular value decomposition", IEEE Trans. nostrum and Meats, vol. 59, no. 11, (**2010**), pp. 3060–3063.

10. Gurpreet Kaur, Kamaljeet Kaur "Image Watermarking Using LSB", International Journal of Advanced
Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.