Architecture for Insertion Unit and Detection Unit by using Digital Watermarking

Poorna Pimpale[1] Prof. Gayatri Naik[2]
[1,2]Department of Computer Engineering
[1,2]Yadavrao Tasgaonkar Institute of Engineering Mumbai, India

Abstract— Digital watermarking is a technique used for video piracy detection. Detection of piracy in video and audio files in AVI RIFF format thus enabling copyright protection. In this paper we have proposed that the video file is watermarked with the copyright information in order to discourage piracy.

Key words: Watermark Insertion, Watermark Detection, Design

I. INTRODUCTION

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 steganographic algorithms, cryptographic techniques and the new era technology watermarking. In this paper digital watermarking technology is used for embedding various types of information in digital content for protecting copyrights and proving the validity of data which is embedded as a watermark.

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 to hide information, for example a number or text, in digital media, such as images, video and audio. The embedding takes place by manipulating the content of the digital data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible. 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. As the watermark is concentrated, the chances of it being prone to damages due to compression etc are more. Several companies work on a watermarking system for copy control in the DVD environment.

II. OVERALL DESCRIPTION

In the proposed paper the video file is watermarked with the copyright information. The copyright information includes data about the vendor, buyer, a serial number and other information. When it is detected that the video is pirated, it is possible to de-watermark the file to retrieve the copyright information. With this information we can trace back to the sources of piracy. In the proposed system the watermark is made invisible. The watermark is spread throughout the image, so it's location cannot be traced easily. The spreading of the watermark also prevents data loss from manipulations like compression etc. Apart from these advantages, the digital watermark in the proposed system can't be erased or overwritten. It is also robust and completely unaffected by common audio or video processing operations. It combines enormous versatility with ease of installation, integration and operation. It offers wide range of applications, including copyright control and broadcast monitoring.

A. Watermark Insertion

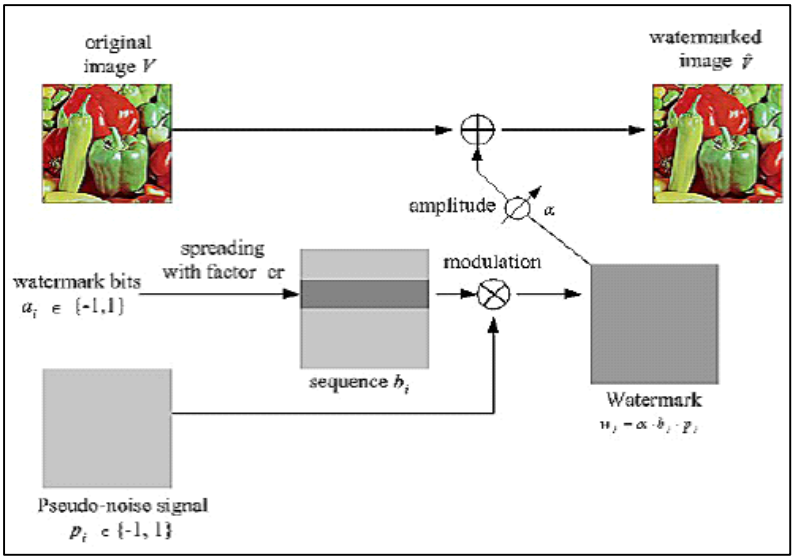

Fig. 1.Watermark Insertion Unit

Watermark Inserting Algorithm is as follows

We first transform the original image in the frequency domain by using DCT transform. Save all coefficient of transformation into vector V.

Spread A by factor crt obtain sequence B using eq. (2). Suppose length of B is L.

- Generate pseudo-noise sequence P as follow: generate first chaotic sequence S1 by using logistic map under an initial value, i1. Length of the sequence is equal to L.
- Then, we set a threshold Two to convert element of sequence (in real value) into binary element (+1/-1), as describe by the following formula:

$$P(i)= \quad 1\ S_l(i)>Tw \ldots\ldots\ldots\ldots(1)$$
$$-1 S_l(i)<=Tw \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

- Next, encrypt embedding position of watermark as follow: we must specify secret positions for embedding watermark. So, we generate the second chaotic sequence,
- S2, by using logistic map under an initial value, i2 (generally ii ≠ i2). Then, convert element of sequence (in real value) into integer by multiplying each element by N× M and then round it toward infinity. We must ensure that there are L different positions of embedding.
- The spread spectrum watermark is embedded into V, except DC value, by using equation (1) and (2) on secret positions.
- Finally, apply inverse DCT to reconstruct the watermarked image.

B. Watermark Detection

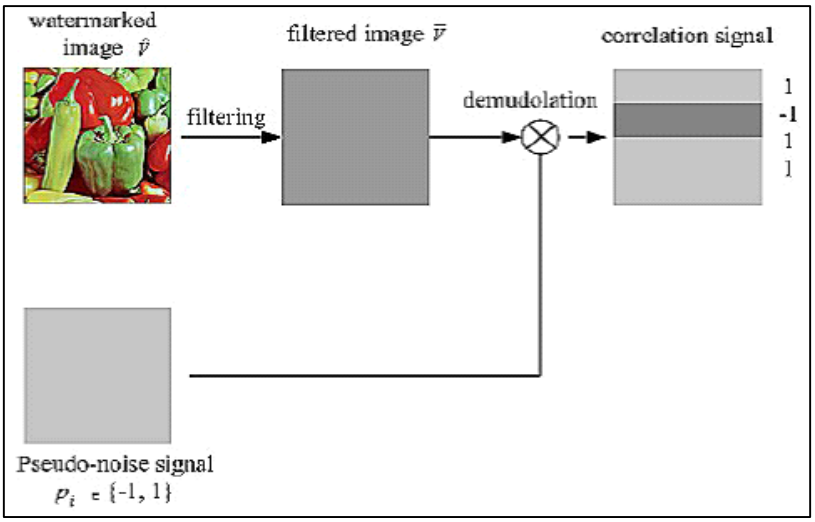

Fig. 2: Watermark Detection or Extraction Unit

Watermark detection involves deciding whether a certain image has been watermarked with a given key.

Watermark Extracting Algorithm is as follows

- To extract watermark from a test image we use the following process:
- We first transform the test image in the frequency domain by using DCT transform. Save all coefficient of transformation into vector Vˆ.
- Generate the same pseudo-noise P that was used in embedding process by using logistic map.
- Generate the same secret position that was used in embedding process by using logistic map.
- Recover bits of the watermark A by using equation. Watermark detection is usually done by correlating the watermarked image with a locally generated version of the watermark at the receiver side. This correlation yields a high value when the watermark has been obtained with the proper key. It is possible to improve the performance of the detector by eliminating original image-induced noise with signal processing.

C. Design

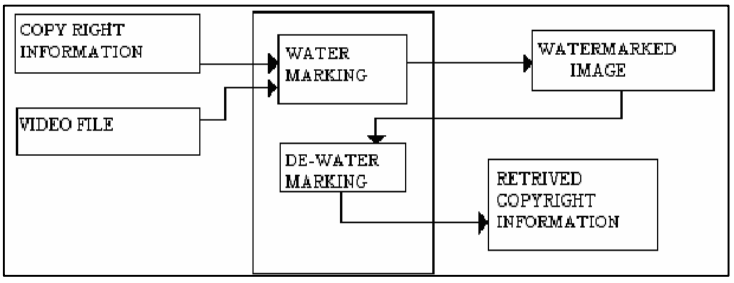

Fig. 3: Block Diagram

As shown in the block diagram, the copyright information in text format along with the video file content in AVI format is given as input to the watermarking module. In this module the textual information is converted compatible to the video file data

and the bits in the video file are altered according to the copyright information. In the de-watermarking module, the copyright information is retrieved from the watermarked file using the key file.

D. Data-Flow Diagram

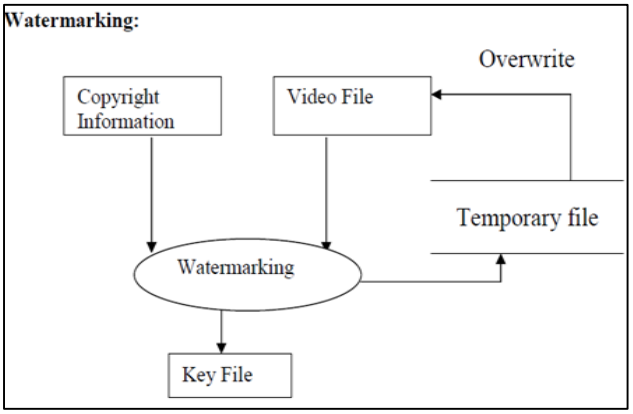

Fig. 4: Data Flow Diagram For Watermarking

The copyright information along with the video content is given to the watermarking module. The copyright information is converted in such a way that is compatible with the video file. The bits in the video file are altered according to the copyright information.

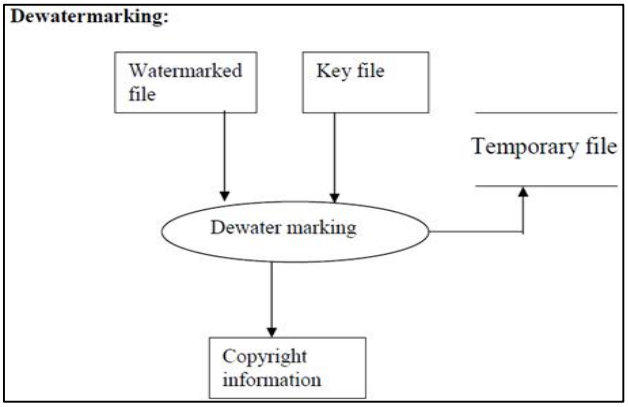

Fig. 5: Data Flow Diagram for De-watermarking

The copyright information can be retrieved from the watermarked file using the key file that is being generated while watermarking the file.

III. CONCLUSION

In this paper the proposed system has used digital watermarking technique to detect video piracy and has overcome most of the major shortcomings of the existing systems. The proposed system renders the watermark invisible and also spreads the entire watermark rather than concentrating it in one place.

REFERENCES

[1] Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference IEEE paper by yujiezhang, 2012.
[2] Cox J., Kilian J. Leighton T, and Shamoon T.,"A secure, robust watermark for multimedia," May 1996.
[3] Tanaka K., Nakamura Y., and K. Matsui, "Embedding secret information into dithered multi-level image," December 1996.
[4] /ieeexplore.ieee.org/
[5] www.watermarkingworld.com