

Comparative Study of Spatial Watermarking of Various Video formats

By

Dinesh Goyal¹, Rishindra Singh², Dr. Naveen Hemrajani³

Scholar, Suresh Gyan Vihar University, Jaipur

Research Scholar, Suresh Gyan Vihar University, Jaipur

Professor, JECRC, University, Jaipur

Dinesh8dg@rediffmail.com, naveenh@gyanvihar.org

ABSTRACT

At the forefront of the information world it is all available in the shape of digital media. Digital watermarking has been introduced to provide authentication owners and copy right protection. Digital video watermarking is the process of embedding a digital code in the digital video sequences. Digital video watermarking is nothing but a sequence of consecutive still images. Over recent years applications based on video, pay-per-view, video-on-demand, video broadcasting are becoming more and more popular, which yield requirements to increase safety in the delivery of video. In this paper, the concept of digital video watermarking, its terminology, principle, properties, applications, and classification is introduced i.e. the detailed technique of watermarking such as Spatial Domain Watermarks (Correlation-Based Techniques, Least Significant Bit Modification), Frequency Domain Watermarks (Discrete Cosine Transform, Discrete Wavelet Transform).

We have taken three video codec i.e. MPEG, IV 50, MJPG of respective video formats MPEG2, H.261 and AVI, which has been watermarked using BITGET video watermarking technique and comparative study among different video formats has been done to provide chaotic map and the efficient video format for watermarking which withstand on the essential ingredients such as fidelity, robustness, use of keys, blind detection, capacity and speed, statistical imperceptibility, low error probability, real-time detector complexity.

1. INTRODUCTION

Today, digital media content (audio or video) can be copied and stored easily and without loss of fidelity. It is therefore essential to use a type of the system that protects the ownership's rights. The majority of content providers will follow production enterprises and use copy protection system called Digital Rights Management (DRM). The encrypted DRM-protected content during transmission and storage on the side of the receiver and therefore copy protected. In addition, the recipient must have a player capable of playing DRM-encrypted content; the biggest drawback is the DRM that once the content is decrypted, it can easily be copied widely used with the utility.

Disadvantages of DRM can be removed by using a different protection Watermark system. Watermark can serve as a part of information hiding called as steganography. Steganographic systems embed hidden information in a content-resistant cover so it does not really stand out. Thus, if someone copies such contents, hidden information copied as well.

Three aspects of information hiding systems contend with each other: capacity, security and robustness. Ability refers to the number of information that can be hidden, security, the ability of anyone to detect hidden information and strength to the resistance to change of the content on the cover of hidden information is destroyed. Watermarking robustness prefer that should not be possible to remove the watermark, without severe deterioration in the quality of content coverage, while requests steganography high security and capacity, i.e., the hidden information usually is fragile and can be destroyed by trivial changes.

Watermark fingerprinting be used in applications usually contain Information on the copyright owner or an authorized recipient of the distributed Multimedia content. It allows back illegally produced copy of the tracking the content, shown in Figure 1.

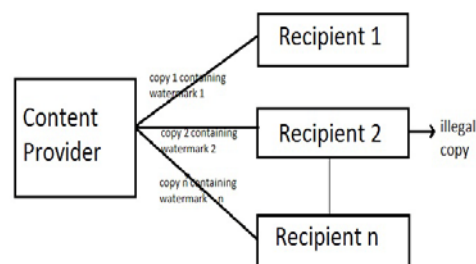


Fig.1 Principle of Fingerprinting

This work focuses on the taking of fingerprints, the watermark embedded in video Sequences. Several watermarking methods are designed, implemented and compared with one another in their visibility and robustness.

Some of the methods are inspired by existing, some are brand new. How to make the perfect method implementations or improve existing methods not the tasks of the paper aims to

compare the methods as they are. One of the processes is chosen as the best choice and for further improvements.

1.1 Overview of Watermarking

Rapid proliferation of multimedia on the Internet takes sophisticated techniques for safe and efficient access to information. There is growing need to discourage unauthorized duplication and use of digital data. With the arrival of digital video, the issues of copyright protection have become more important, such as the duplication of digital video does not result in a decrease in the intrinsic quality normally suffered by the analog video. Techniques of steganography, data hiding, data integration and watermarking are used for invisible information that incorporates a host of data, with the intent information is stored / transmitted together with data retention host secret information. The major difference between steganography and water marks steganographic is that the methods rely on the fact that secret communication is only a point to point communication and trust among the parties that are unfamiliar to others. Therefore, methods of steganography are not designed to be robust against attack attempts. In watermarking methods the existence of integrated information is unknown to unauthorized persons have access to the data, and may grope unlawful attacks.

1.2 Video Watermarking

Digital watermarking for still pictures has been studied extensively. But today, the growing popularity of Internet-based applications such as multimedia, wireless video, video recorder, video on demand, set-top boxes, video and video conferencing has increased by secure video distribution demand. It appears each image watermarking technique may be raised to video watermarking, but in fact the video watermarking technique must meet further challenges such as image watermarking method. Some of the video characteristics that impact watermarking include:

- High correlation between successive frames. If Independent watermarks are embedded in every frame, an attacker could run average frame to remove significant portions of the watermark embedded.
- Applications, such as monitoring of transmissions require real-time processing, and therefore should have little complexity.
- Imbalance in among the regions of motion and real estate.
- Watermarked video footage is very susceptible to malicious attacks such as average frame, frame exchange, statistical analysis, digital-to-analog (AD / DA) conversions and lossy compressions.

1.2.1 Applications of Watermarking

Watermarking techniques are often evaluates on the common characteristics robustness, tamper resistance and fidelity. However, can often be deceptive examine these characteristics without careful examination of the application. The most important applications are copy control, broadcast monitoring, fingerprint, video authentication, copyright protection

- Copy Control: It's not possible to respond to the embedded recording and playback devices signals. In this manner, a recording apparatus of a recording signal when inhibit it detects a watermark that indicates the receptacle is prohibited. Here

watermarking supplemented the available technologies in which the secured information header and prevents copying of the data.

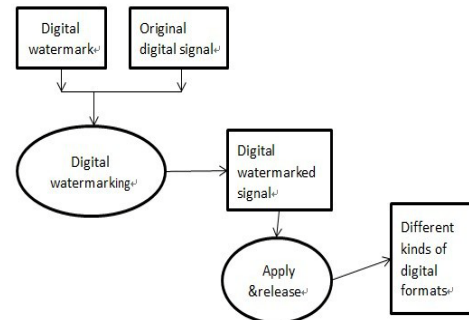


Fig.2 Workflow of digital watermarking applications

- Broadcast Monitoring: Many useful products are distributed via television Network. As a result, a broadcast control system, build by check all broadcast channels. We may use watermarking for broadcast monitoring by a unique watermark in each video clip or sound before the show. Automated monitoring stations can receive broadcasts and look for these Watermarks, identifying where and when each frame appears.
- Fingerprinting: Electronic delivery of content allows each copy distributed be customized for each recipient. This permits a unique watermark which is embedded in each copy of the customer, such as customer name or ID. This will enable distribution companies to trace the source of illegal copies in the event of a leak. Another important topic of illegal copying new projected on the big screen with a video camera hold movies. A watermark may indicate the time that the film, the date and time of the presentation to be embedded identified. When the illegal copy is produced by a video camera is located, the watermark is extracted and film, the fault is identified.
- Video Authentication: There are lots of applications in medical imaging and right where it is important to get the contents of the temperature. The authentication can be done by storing the signature in the header field, but this title will still be vulnerable to tampering. One preferred approach to this problem is to embed the signature directly into the watermark image. This will ensure that the signal with the image on the left and edited image is propagated to the watermark.
- Copyright Protection: The underlying strategy is to embed watermarks, identifying the holder of the copyright of digital media data. The legal owner can show the watermark in the case of a dispute. Therefore, the watermarking algorithms are required for services not reversible protection of copyright, particularly in cases of multiple ownership problems.

1.2.2 Types of Digital Watermarks

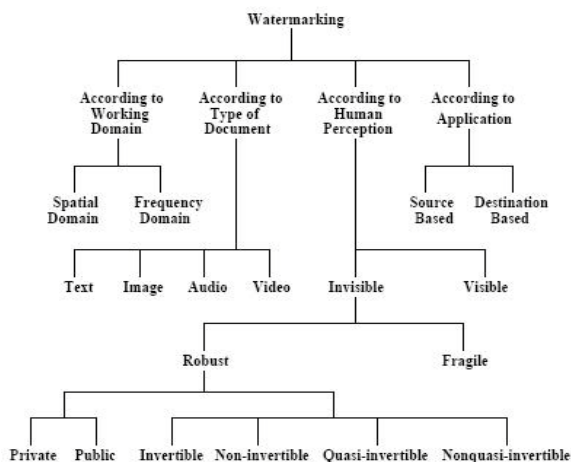


Fig.3 Watermarking Techniques

Watermarks and watermarking techniques can be divided into various categories in various ways. Watermarking techniques can be split into four categories according to the type of document being watermarked as follows: [1]

2. DIGITAL VIDEO WATERMARKING

Several digital watermarking schemes were proposed in literature for still images and video. Most of them operate on uncompressed video, whereas others embed watermarks directly in compressed video. Recently, researchers tend to study techniques for video watermarking that is robust and invisible. Such systems can be differentiated in terms of the domain that the watermark is embedded or detected, real-time performance, their capacity, the degree in which are incorporated the three axes, and their resistance to particular types of attacks. A map of the classification techniques of existing video watermarking is presented in Figure 8. They can be split into three major groups based on domain in which the watermark is incorporated, are territorial.

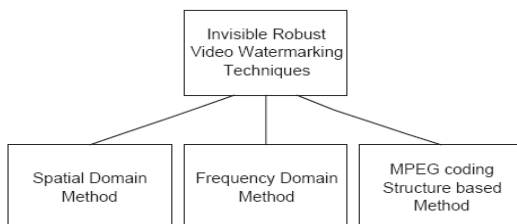


Fig. 4 Classification map of existing digital video watermark techniques domain,

Spatial Domain Watermarks

First, we examine techniques for video watermarking in the spatial domain. Algorithms of this class typically share the following features:

- Watermark applied to the pixel domain or coordinate.
- No changes are applied to the host signal during watermark embedding.
- Watermark was derived from the message data by using spread spectrum modulation.
- Conjunction with the host signal operates on simple tasks within pixel domain.

- The watermark can be recognized by correlating the model provided by the received signal.

The different methods allow watermarking in the spatial domain.

Correlation-Based Techniques

Another technique for embedding watermark is to exploit the correlation properties of additive pseudo-random noise models as applied to an image [4]. A pseudo-random noise (PN) pattern $W(x, y)$ is added to cover the image $I(x, y)$, according to equation as shown below in equation 2.1:

$$I_w(x, y) = I(x, y) + kW(x, y) \quad (2.1)$$

In Equation 2.1, k indicates a gain factor, and resulting watermarked image I_w . By increasing k enhances the robustness of the watermark at the expense of image quality watermarked. To retrieve the watermark, the same algorithm for generation of pseudo-random noise is seeded by using the same key, and correlation among the image watermark and noise pattern is calculated. Whether the correlation exceeds a certain level T , the watermark is found, and a single bit is set. This method may be easily extended to a multi-bit watermark; this is done by dividing image into blocks, and executes the procedure described above independently on each block. This core algorithm can be enhanced in several ways. First, the concept of threshold used to determine a logical '1' or '0' can be deleted by acting two models of pseudorandom noise separated. A model is designated as a logical '1' and the other '0'. The procedure described above is then performed once for every model, and uses the model with highest correlation result. This increases the chance of correct detection, even though the image has been subjected to an attack.

Least Significant Bit Modification

The simplest example of a spatial domain watermarking technique that does not rely on the correlation method is the LSB (least significant change). If every pixel in a gray level is represented by an 8-bit value, the image easy to cut in planes 8 bits.

As the Scheme of the least significant bit does not contain any meaningful information visually can be easily replaced by an enormous amount of bits of watermark. The most sophisticated watermarking algorithm that makes use of LSB modification found in [5]. In fact such watermarking techniques are not very robust for processing technique because the LSB plane can be easily replaced by random bits, efficiently removing the watermark.

There are plenty algorithms for invisible digital watermarks. The simplest algorithm is Least Significant Bit (LSB) Insertion, in which each 8-bit pixel's least significant bit is overwritten with a bit from the watermark.[6] In view of the extremely high channel capacity by using the whole cover for the transfer in this method, a smaller object can be embedded repeatedly.[6].

In digital image, information is added directly into each bit of the image information, or the more crowded areas of an image computed to hide such messages in less perceptible parts of an image. Two general techniques were introduced, to hide data in the spatial domain of images. These procedures were on the pixel value of the least significant bit (LSB) changes.

The algorithm proposed by Kurah and McHughes [7] to embed in the LSB and it was known as image downgrading [8].

An example of the less predictable or less perceptible is Least Significant Bit insertion. This section shows how this works for an 8-bit grayscale image and possible effects of the change of such image. The principle of integration is quite simple and effective. If we have a grayscale bitmap image using 8 - something we would need to read in the file and then data in the least significant bits of each pixel in each 8-bit pixel

Video Formats

Format Container: .avi, .mp4, .mov, .ogg, .flv, .mkv, etc.			
Video codec:	Audio codec:	Captioning, Video description:	Metadata:
H.264, VC-1, Theora, Dirac 2.1, H.263, etc.	AAC, WMA, Vorbis, PCM, etc.	SAMI, SMIL, Hi-Caption, CMML, DXFP, 3GPP TS 26.245, MPSub, etc.	Author, Title, Location, Date, Copyright, License, etc.

MPEG 2

Project in MPEG-2 was approved in November 1994, and was the extension of MPEG-1, which is aimed at covering the cost of higher bandwidth for large images and higher quality. MPEG-2 applications for digital television transmission usually require a speed of 15.4 Mbps (up to 100 Mbps), as the digital high-definition television (HDTV), interactive storage devices (ISM) designed and cable TV (CATV) (Sikora, 1997, Ali, 1999).

MPEG-2 is composed of different parts, of which the most important for us is part of the video. This standard defines a compressed video bitstream and describes how this can be decoded. It is important to understand that it cannot describe how to take an input image and compress do bitstream MPEG-2 - a specification of the programmer. Encoder designer has complete freedom to use, what aspects of the standard and how to use them. Therefore, it is best with the MPEG-2 to be selected as a toolkit for video compression, which provides the right tools for different applications think.

H.261

H.261 standard was developed by ITU (International Telecommunication Union), for data rates that are multiples of 64 kbps. In this temporal prediction for motion compensation is used. Two resolutions are supported by H.261, an image size of 352 × 288 in Common Interface Format (CIF) and an image size of 172 × 144 (Bernd et al, 1995. Roden, 1996; Mee-Hye et al., 1998) in Quarter CIF (QCIF).

AVI

Audio Video Interleave – a Microsoft multimedia container format introduced in 1992 as part of its Video for Windows technology. AVI files can contain audio and video data in a standard container and deliver synchronous video / audio playback. Most of the AVI files also use file format extensions OpenDML, forming AVI 2.0 files.

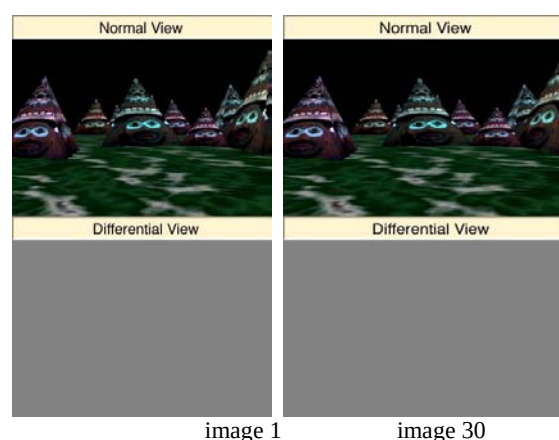
Some people consider AVI obsolete, as there are considerable costs to use it with popular MPEG-4 codec which apparently unduly increase the size of the files. Nevertheless, it remains popular among the community of file-sharing - probably because of its high compatibility with video editing software and the existing breeding, such as Windows Media Player.

AVI is a derivative of Resource Interchange File Format (RIFF), which splits the a file's data into blocks, or "chunks". Each "chunk" is identified by FourCC tag. AVI file takes the shape of a single chunk in a RIFF file format, which is then divided into "blocks" mandatory and one voluntary "chunk".

3. EXPERIMENTS AND RESULTS

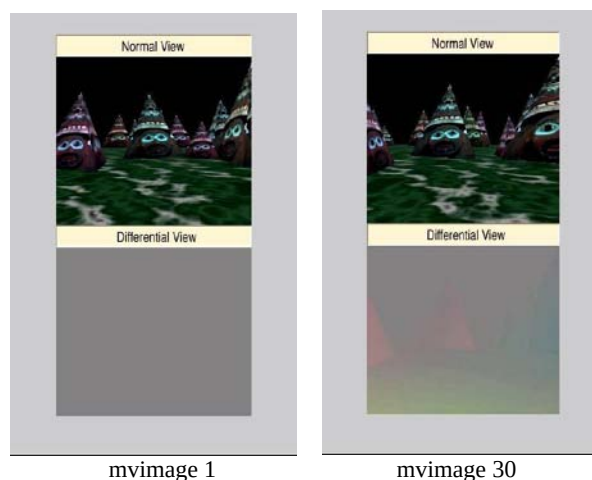
Scenario 1, This one is the original video on which watermarking has to be done i.e. MPG video named as job.mpg having following detail

Size : 637 kb
 Length : 0.1 sec
 Frame Width : 352
 Frame Height : 544
 Data rate : 5404 kbps
 Total bitrate : 5404 kbps
 Frame rate : 30 frames/sec



Scenario 2, Here Selective Watermark is performed on MPEG 2 video is move.m2v file having M2V video format.

Size : 160 kb
 Length : 0.3 sec
 Frame Width : 176
 Frame Height : 176
 Data rate : 400 kbps
 Total Bitrate : 400 kbps
 Frame rate : 25 frames/sec



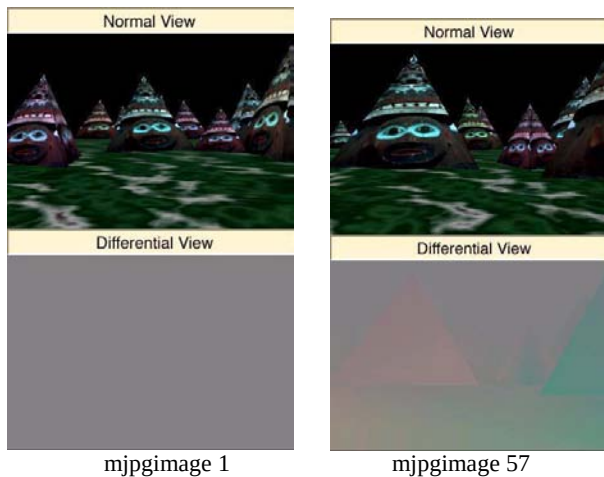
Elapsed time for watermarking

18.146 sec

Elapsed time for coding 134.128 sec

Scenario 3, Here Selective Watermark is performed on H.261 video is shuttle_out.avi file having AVI video format.

Size : 1.11 mb
Length : 0.1 sec
Frame Width : 352
Frame Height : 544
Data rate : 4924 kbps
Total Bitrate : 4924 kbps
Frame rate : 30 frames/sec



Elapsed time for watermarking 13.7977 sec
Elapsed time for coding 3.1502 sec

Scenario 4, Here Selective Watermark is performed on IV 50 video is 724.avi file having AVI video format.

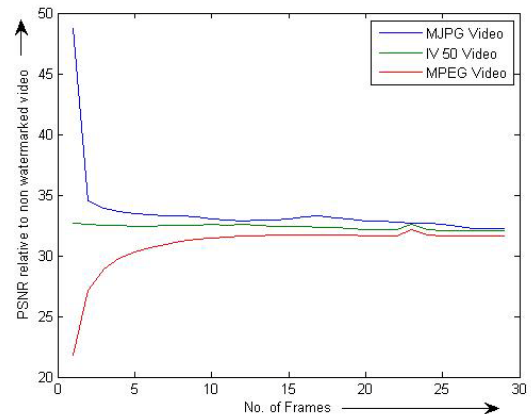
Size : 553 kb
Length : 0.1 sec
Frame Width : 516
Frame Height : 632
Data rate : 2417 kbps
Total Bitrate : 2417 kbps
Frame rate : 30 frames/sec

4. RESULT ANALYSIS

In this the results of three types of the video formats are watermarked using BIT GET watermarking technique and compared with their respective results.

The results shown in previous part are taken after performing chaotic map based selective watermarking on video.

1. In this work the MJPG video is represented by the blue line where the normal input video is watermarked using selective watermarking technique i.e. BITGET technique that produce chaotic map.
2. The IV 50 video is shown by green line that has been watermarked by BITGET watermarking technique for chaotic map.
3. For MPEG video we have red line and has been watermarked by BITGET method to give chaotic map.



The above line shows the watermarking variation among the three video, the blue line shows MJPG video, green shows IV 50 and red one shows MPEG video.

As output comes, it demonstrate that the PSNR of starting frames of MJPG video are higher but as the frames increases in the case of PSNR still the performance of MJPG video is better than the IV50 and MPEG video.

5. CONCLUSION AND FUTURE WORK

Digital Watermarking has been the need of the hour in all digital multimedia applications in order to ensure confidentiality and integrity of the content shared online in the present era. Various Digital Watermarking techniques exist namely, spatial domain & Frequency domain which can further be categorized in various sub types.

Multimedia can be a image, audio or a Video, which has been time and again watermarked using above techniques, but results of the same vary as per the type and quality of multimedia.

Video is the most shared multimedia in present scenario, Many video codecs also exist in present era for ensure better quality of delivery but while ensuring their integrity and confidentiality the quality is deteriorated.

In this work an attempt has been made to analyze the performance of various video codecs when watermarked with spatial watermarking.

As the results show that better video quality can help to retain better quality and thus MJPG is better than IV50 or MPEG format as it is only stand compressed while IV50 or MPEG are more compressed thus they show poor performance in terms of spatial watermarking.

It can thus be concluded that high compressed codecs like MPEG and further are better adapt to frequency watermarking than that of spatial watermarking, because spatial watermarking creates impact on image data.

Spatial Watermarking is better for uncompressed videos and Frequency watermarking is better for compressed video.

In future the same work can be carried out with frequency watermarking in different video formats and also a comparative study may be done for similar type of video for different type of watermarking techniques.

6. REFERENCES

- [1] Hal Berghel, A. et. Al. "Watermarking Cyberspace", Comm. of the ACM, Nov.1997, Vol.40, No.11, pp.19-24.
- [2] [Kirthika, A.](#) et. Al. "Different video watermarking techniques and relative study with reference to H.264/AVC", ICCIC,2012 IEEE International Conference ,
- [3] Sanjana Sinha, A. et. Al., "Digital Video Watermarking using Discrete Wavelet Transform and Principal Component Analysis", International Journal of Wisdom Based Computing, Vol. 1 (2), August 2011
- [4] R. Aarthi, A. et. Al. "Modified LSB Watermarking For Image Authentication" International Journal of Computer & Communication Technology (IJCCT) ISSN (ONLINE): 2231 - 0371 ISSN (PRINT): 0975 -7449 Vol-3, Iss-3, 2012
- [5] Yeuan-Kuen Lee1, A. et. Al. "An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding" Springer-Verlag Berlin Heidelberg 2009
- [6] G. W. Braudaway, A. et. Al. "Protecting Publicly Available Images with a Visible Image Watermark", Proc. SPIE Conf. Optical Security and Counterfeit Deterrence Technique, Vol. SPIE- 2659, pp.126-132, Feb. 1996.
- [7] Frank Hartung, A. et. Al. "Spread Spectrum Watermarking: Malicious Attacks and Counterattacks". Security and Watermarking of Multimedia Contents, 1999.
- [8] G. Langelaar, A. et. Al. "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol. 17, pp. 20-43, Sept. 2000.
- [9] H. Kinoshita, "An image digital signature system with ZKIP for the graph isomorphism", in Proc. IEEE Int. Conf. on Image Processing, vol. III, Lussane, Switzerland, Sept 16-19,1996.
- [10] Max Sobell"LSB Digital Watermarking", CPE 462
- [11] Dr. Martin Kutter A. et. Al. "Digital Watermarking Technology", AlpVision, Switzerland, pp 1 – 4
- [12] Brigitte Jellinek, A. et. Al. "Invisible Watermarking of Digital Images for Copyright Protection" University Salzburg, pp. 9 – 17, Jan 2000.