

DIGITAL WATERMARKING SCHEME USING VIDEO WATERMARK TECHNIQUES

Ankita Amburle

Department of Computer Engineering, Savitribai Phule Pune University
'Rajani Anant', Kacheri road, Tal-Mangaon Dist raigad(402104), India

ankita.amburle@gmail.com

Abstract— The effective purpose a watermark should adhere to a few requirements. In specific, it should be robust, and transparent. Due to the replicable nature of video many illegal copies of original videos can be produce. So its demand to deliver methods for preventing illegal copying. In this paper identifies a new digital watermarking approach for copyright protection of video based on wavelet transformation. Very first, the motion part of color video is detected by scene change analysis, and then applying 3D wavelet transformation over a detected motion part 10 sub hands of wavelet coefficients are obtained. Watermark is embedded into selected wavelet coefficients. In extraction step, the original video is not needed, namely, blind detection. The resultant watermarking scheme is used for public watermarking applications where the original video is not available for watermark extraction. The robustness of proposed method against various kinds of attacks such as median filtering, frame drop, frame averaging, frame swapping and there are lots of lossy compression including MPEG-4, MPEG-2, and H.264 shows the fidelity of our claim

Keywords— Wavelet transformation, frame drop, filtering, wavelet coefficient.

I. INTRODUCTION

In the recent information age, the rapid development of various communication techniques, the exchange of digital multimedia content becomes more comfortable. Digital watermarking means it is a technology for embedding various types of information or data in digital content. This information could be the copyright, logo, signature or any other useful information. The detection of watermark from the watermark data can then prove the ownership or the copyright of the host data. According to the range of applications, digital watermarking can be classified into image watermarking, audio watermarking, video watermarking etc. By the basis of domains which watermarking processed in, it can be classified as the spatial domain and the transform domain watermarking. The transform domain scheme which is usually more robust than the watermarking scheme in the spatial domain has attracted more attention. According to the history of the watermarking development, it can also classify as the first and second generation. The first generation watermarking is the routine which uses pixels, frequencies or other transform coefficients to embedding the watermark. The second generation watermarking is the routine involves the notion of perceptually significant features in the data.

The basic requirements of digital video watermarking are invisibility, robustness and capacity.

1. **Invisibility:** A degree that an embedded watermark remains unnoticeable when a user views the watermark digital media. the data should embed the watermark in the regions of the video frame in which imperceptibility is least affected.
2. **Robustness:** The resilience of an embedded watermark against being removed by incidental and intended attacks. There are having some attacks on videos are filtering, adding noise, compression, frame dropping, frames averaging and frame swapping.
3. **Capacity:** The amount of information or data that can be reliably be hidden when the scheme provides the ability to change digital data.

A. Principle of Digital Watermark

A watermark on bank notes has a different transparency than the rest of the notes when a light is focused on it. However, this method is useless in the digital world. Currently there are various methods for embedding digital watermarks. They all digitally write desired information directly onto images or audio data in such a manner that the images or audio data or information are not damaged. Embedding watermarks should not result in a significant increase or reduction in the original data.

B. Materials Suitable For Watermarking

Digital watermarking is suitable for any type of digital content, including still images, animation, and audio data or information. It is easy to embedded watermarks in material that has a comparatively high redundancy level ("wasted"), such as color still images, animation, and audio data; however, it is difficult to embed watermarks in material with a low redundancy level, such as black-and-white still images. To resolve such a problem, we developed a technique for embedding digital watermarks in black-and-white still images and a software application that can effectively embed and detect digital watermarks.

II. VIDEO PRE-PROCESSING

Applying independent watermarks to each frame presents a problem. If regions in each video frame remain little or no motion frame after frame. These motionless regions may be

statistically compared or averaged to remove the independent watermarks. From other point of view, dividing the video based on scene-change detection will not be useful if the video changes occur rapidly or contains too many different short scenes. In addition, if the video contains long motionless scenes, the algorithm will face some difficulties.

Therefore, in this experiment, we decided to place the watermark into motion scene frames. In order to detect the motion part of video, a heuristic and simple method is delivered, it means:

```

n
if  $\sum_{i=1}^n \text{His}(F_j(i)) > \text{th}$ 
  F'(i)=motion frames
Else if
  F'(i)=motionless frames
End if

```

For this purpose only the histograms of red components for all frames are utilized. In this method I is the number of frames, j is the red component of frames and th is the threshold. So by considering a threshold of 3800, a scene change is detected and adaptive frames for embedding the watermark will be achieved.

III. DIGITAL VIDEO WATERMARKING:

Video Watermarking is one of the most popular techniques among the various Watermarking techniques currently in uses. This is because maximum occurrences of copyright infringement and abuse happen for video media contents.

IV. THE PROPOSED WATERMARKING ALGORITHM

A. Watermark Embedding Process

Step 1: After detecting motion part of video or stream, a three dimensional wavelet in three levels is applied over these frames.

Step 2: The Three dimensional coefficients of HL, LH and HH are chosen for embedding the watermark. Coefficients of LL are not watermarked; video energy is concentrated on lower frequency wavelet coefficient. If they are altered, it will effect on perceptual quality.

Step 3: A spread spectrum technique is used to spread the power spectrum of the watermark data into selected 3D wavelet coefficients. At first, three sets of pseudo random numbers based on Mersene-Twister algorithm which is proposed by Mastsuoto and Nishimura are created. That is each set of pseudo random numbers are generated in order to insert the watermark into the specific wavelet sub bands of HL,LH or HH.

Following algorithm shows embedding process

```

If  $I(i,j)=0$  then
   $C'v(i,j,k)=Cv(i,j,k)+\alpha.Wv(i,j,k)$ 
Else if
   $C'v(i,j,k)=Cv(i,j,k)$ 
End if

```

Where α is an intensity factor, $Cv(i,j,k)$ is the 3D-DWT coefficient of motion part frames, $C'v(i,j,k)$ is the watermarked 3D-DWT coefficient of motion part frames, $I(i,j)$ is the binary watermark and $v \in \{HL,LH,HH\}$.

Step 4: After embedding the watermark, a 3D-IDWT is performed on the motion part frames.

B. Watermark detection process

Step 1: Performing the 3D-DWT on motion part frames, that is, 2D-DWT on each frame and 1D-DWT along temporal axis over frames.

Step 2: Choosing the three dimensional coefficients of HL,LH and HH which are decomposed by three levels wavelet.

Step 3: Generating three sets of pseudo random numbers based on Mersenne-Twister algorithm using the same key which is used in embedding Process.

Step 4: Calculating the correlation between the extracted coefficients and their relative Pseudo-random numbers gives the hidden watermark:

If $\sum(\text{corr}(ECv(i,j,k),Wv(i,j,k))) > \text{th}$

Watermark is detectable

End if

C. Uncompressed Domain Watermarking For Video

For a Spread spectrum scheme is used to embed the watermark data into the raw uncompressed video. Here, watermark data is considered as narrow band signal and video is considered as wide band signal. Narrow band signal is spread for increasing redundancy and then modulated with binary pseudo noise sequence. This modulated sequence is called spread spectrum watermark, which is added linearly to the video data. The reason for adding pseudo-noise is to prevent detection and attack of the watermark data.

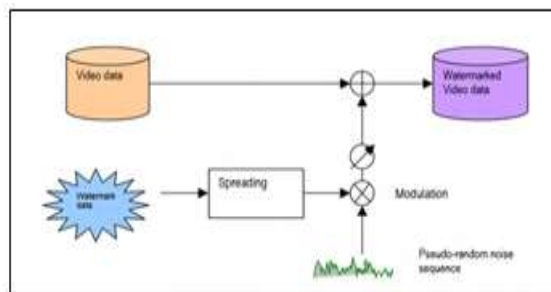


Fig:1 Spread spectrum watermark embedding in uncompress domain

Any authorized detector, which has the knowledge of the pseudo-random signal that was used for watermark embedding purpose, can recover the watermark. The steps are shown in figure 2 below.

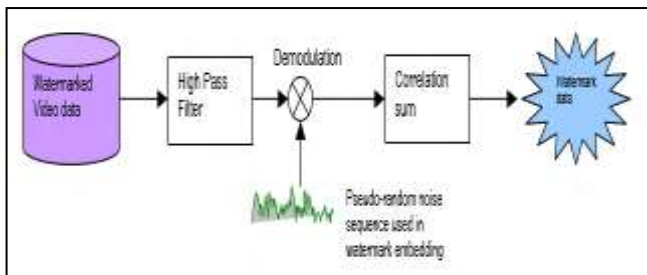


Fig:2 Spread spectrum watermark recovery in uncompressed domain

D. Spread spectrum watermark recovery in uncompressed domain

Compressed domain Watermarking for video Due to high bandwidth requirement, video is usually carried in compressed domain. Different encoding methods like H.261, H.263, MPEG-2, and MPEG-4 are used to compress video. Video data Spreading Watermark data Watermarked Video data Pseudo-random noise sequence Modulation Watermarked Video data High Pass Filter Demodulation Correlation sum Watermark data Pseudo-random noise sequence used in watermark embedding All of them use hybrid coding, which is motion compensated prediction-based algorithm. Encoding methods may vary from simple to complex depending on target bandwidth required. The computation requirement is almost equal to (if not more) a decoder. Hence, algorithm chosen should be robust enough to withstand different kinds of attack.

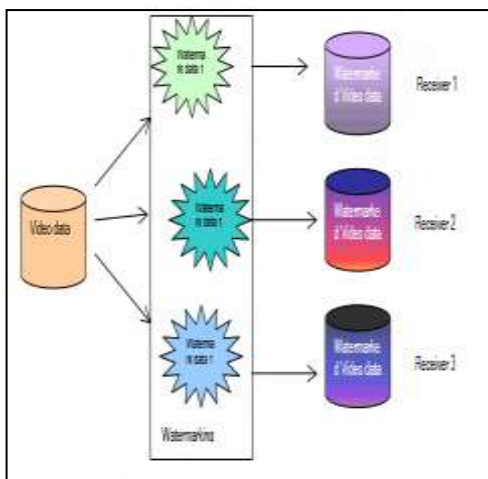


Fig:3 Watermarking for video on demand scenario

V. CONCLUSIONS

Digital watermarking holds significant promise as one of the keys to protecting proprietary digital content in the coming years. Also the different techniques help us for security purpose. It focuses on embedding information inside a digital object such that the embedded information is inseparable bound to the object. Tampering with the watermark or otherwise altering a watermarked object should always be detectable, and attempting to remove a watermark from its object should cause to be that object useless. Currently, watermarking suffers from several drawbacks that prevent it from providing the creators of

digital content with a solid guarantee of copyright protection.

REFERENCES

- Ingemer J. Cox: Digital Watermarking and steganography. Morgan Kaufmann, Burlington, MA, USA, 2008
- T. Jayamalar, DR. V. Radha, "survey on Digital video Watermarking techniques and attacks on watermarks" International journal of engineering Science and Technology, Vol. 12, 6963-6967, 2010.
- E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," ACM Multimedia and Security Workshop 2004.
- P.W. Chan and M. Lyu, "A DWT-based Digital Video Watermarking Scheme with ErrorCorrecting Code," Proceedings Fifth International Conference on Information and Communications Security (ICICS2003), Lecture Notes in Computer Science, Springer, Vol. 2836, pp. 202-213, Huhehaote City, Inner-Mongolia, China, Oct. 10-13, 2003.
- B. Vassaux, P. Nguyen, S. Baudry, P. Bas, and J. Chassery, "Scrambling technique for video object watermarking resisting to mpeg-4," Proceedings Video/Image Processing and Multimedia Communications 4th EURASIP/IEEE Region 8 International Symposium on VIPromCom, pp. 239-244, 2002
- B. Mobasseri, "Direct sequence watermarking of digital video using mframes," Proceedings International Conference on Image Processing (ICIP-98), Vol. 3, pp. 399-403, Chicago, Illinois, Oct. 4-7, 1998.
- K. Su, D. Kundur and D. Hatzinakos, "A novel approach to collusion-resistant video watermarking", Proceedings of the SPIE, vol. 4675, pp. 491-502.
- B. G. Mobasseri, "Exploring CDMA for watermarking of digital video", (1999) proceedings of the SPIE, vol. 3675, pp. 96-102.

AUTHORS

Author-Ankita Amburle Completed her BE Computer From Modern Education Society College of Engineering, Pune University.

Email Id: ankita.amburle@gmail.com