

Digital Video WaterMarking System using Audio Information of Image Discrete Frequency on improved security through Pre-Processing

<p>Kyung-Sang Sung Computer Science Department KyungWon University of Sung-Nam city Kyung-Gi Province, Korea</p>	<p>Jung-Jae Kim Computer Science Department Soongsil University of Dong-Jak Gu Sang-Do Dong, Seoul</p>
<p>Hae-Seok Oh Computer Science Department KyungWon University of Sung-Nam city Kyung-Gi Province, Korea</p>	<p>Moon-Seog Jun Computer Science Department Soongsil University of Dong-Jak Gu Sang-Do Dong, Seoul</p>

Abstract - Digital watermarking is a technique wherein copyrights are protected by inserting difficult to separate indications such as video, audio, or texts to the content, which is a method to prevent illegal distribution, or copying of the product without proper authorization from maker or owner. In this research, unlike the existing image watermarking method wherein watermark is done to the frame itself, a model which extracts audio information within the moving picture, inserts image watermark into the extracted audio information which represents the owner, then combines original image together with digital audio watermark image. Also, suggests a model that improves security of watermark itself, by conducting pre-processing of watermark.

Keywords: Watermark, DRM, Image Discrete Frequency.

1 Introduction

These Together with fast growing development of computer and network technology, and increase in multimedia data, numerous commercial dealings on digital contents are being made on-line. For information business, and strengthening of company's competitiveness, many aspects such as society's economical cultures are digitalized, and digitalization of information is being developed even at this moment, thus it is forecasted that 80% of the contents will be digitalized by the year 2006. In line with this, creation of high-speed communication network, multimedia technology and rapid development of internet is leading information transition towards user-focused multimedia. However, as this information internet-based multimedia are being distributed as surrounding environments are developed, original digital products are illegally copied and distributed infinitely causing serious problems in the society, and in order to counteract such violation of copyrights, many techniques and methods have been suggested. Currently, many technologies such as

DRM(Digital Rights Management) have been studied to protect the contents, and among them is a method called Watermarking where specific code or pattern is inserted into the content itself to prove copyrights, and to prevent illegal exposure of the content.

In Watermarking technique, one of the methods to protect copyrights of digital data, watermark representing copyrights of digital data is extracted and inserted into digital image or video, which is not easily detected human vision or hearing, which can still be detected after various attacks such as editing. It is a technique provided to the user using the data, to protect the rights of ownership. The indication inserted is called Watermark, and this has several interesting features. Firstly, inserted watermark should not be detected by human. Meaning, inserting watermark to the multimedia should not degrade or affect the quality of the contents itself. Secondly, even if the inserted watermark gives changes to the contents, it should not receive any changes. If changes to the content cause damages or removal of the watermark, it can not protect the rights of authorship on the contents.

In current digital video watermarking method, moving pictures are treated as a group of continuous frames, and frequency components of each frame are slightly adjusted. In such case, if direct alterations are made on the frame, it could lower the quality of the picture, thus this study used the characteristic that moving picture is composed of image and audio, to present a method where digital audio image watermark representing copyrights are inserted into extracted audio information, and watermark is inserted into extracted and separated image information after which the 2 are combined. Also, in order to improve security of watermark it self, pre-processing of watermark is suggested. Since recent events on illegal copy and distribution of MP3 audio files are causing great issue,

watermarking technique on audio data must be mastered immediately.

2 Related Studies

Basically, Digital watermark have four features. First, Digital watermark should not be visible, and should not lower the quality of the picture. Second, inserted in order to present the copyrights of the images, should be able to survive various processes such as compression, enlargement/reduction, D/A conversion, and A/D conversion. Third, As watermark is searched, the person's copyright must be clearly presented. In other words, watermark extraction should be convenient depending on the owner. Fourth, Even if insertion method of watermark is widely known, as long as related parameter values are unknown, illegal attempts to delete watermark should be impossible.

2.1 Digital watermarking for authentication and integrity

Watermarking is used not only for protection of multimedia data, but also for authentication and integrity of such data. If multimedia is used for legal purposes, medical purposes, and industrial purposes, the creator of such image and whether such media was tampered or not can be checked at the same time. As a main example of method that confirms authentication and integrity of image, there is a public-key watermark method of Ping Wash Wong presented in 1998 using public-key secret code algorithm. If keys improper for existing system are used to check for watermark, or if image was enlarged or parts of the images were cut, noise is given off instead of the image to provide integrity and authentication.

2.2 Classification according to location of watermak insertion

In technological aspect, location of watermark insertion provides the basis for classification. Depending on location of insertion, watermark can be inserted on space area and frequency area.

In space area method, data such as images are analyzed in space aspect, data to be inserted are scattered within that space to make it difficult to identify, then direct alterations are made to image pixel value to complete watermark insertion. In this method, although insertion of watermark is easy, it is relatively weak on processing images such as loss-compression (JPEG) and filtering.

In frequency method, multimedia data are converted into frequency type signal, after which watermark is inserted. In other words, watermark is inserted in values of the frequency area. Ordinarily, it is a data conversion method, using techniques such as DCT (Discrete Cosine

Transform), and FFT (Fast Furie Transform), DWT (Discrete Wavelet Transform). In this method, values for watermark to be inserted are distributed within the entire data, and once such watermark is inserted it is not easily removed by ordinary attacks.

2.3 Watermarking audio data

Adapting human's sense of hearing, this method is strong against outer attacks, and many methods that do not lower the quality of the audio are mentioned.

1) Lower beat adjustment method

Watermark is inserted to each audio sample's LSB (Least Significant Bit), which is commonly used for data sending, receiving mode without any jarring noises. Data sampled at 1KHZ sends off 1kbps data. For noises in sending/receiving channel or compression of re-sampling, extraction of watermark is quite difficult thus additional technology can provide security against outer attacks.

2) Phase cipher method

As a method that takes into consideration human's dull sense towards phase changes, where phase is fabricated and data is inserted, watermark signal is added to frequency area. Watermark extraction is possible if device that detects length of frequency area and starting point, and the audio file are present. Depending on sound data, it can send in various ranges from 8bps~32bps.

3) Diffusion spectrum method

In order to insert watermark, low value should be added to wide range, and J.Cox's diffusion spectrum method is the technology which uses such technique. In diffusion spectrum method, random sequence is used as watermark. The sequence has identical distribution function, and since it is equally distributed among all ranges of frequency, thus it is a method that can be used effectively.

4) Echo masking method

Here, echo data is inserted to audio signal and data is masked with the parameter (initial amplitude, decay ratio, offset). Offset refers to delay created between 2 notes when audio signal and echo notes are combined. Although human's sense of hearing is more sensitive than sense of vision, hearing can not detect a short echo signal, thus in this method echo signal with different delay are inserted.

3 Proposed watermarking technique

Digital watermarking is an insertion technique where specific data that represents copyrights and ownership of

multimedia contents such as audio, video, image and texts are inserted which is not clearly differentiated with human's sense of hearing and vision.

3.1 Design of the propose watermark system

Such techniques are intended to provide basis for exercising rights of ownership by extracting such specific data, when original ownership and copyrights need to be checked during distribution procedures. Suggested watermarking techniques took into consideration the characteristic that moving pictures are made up of image and audio data, and also on sense of hearing sensitive to high frequency audio range

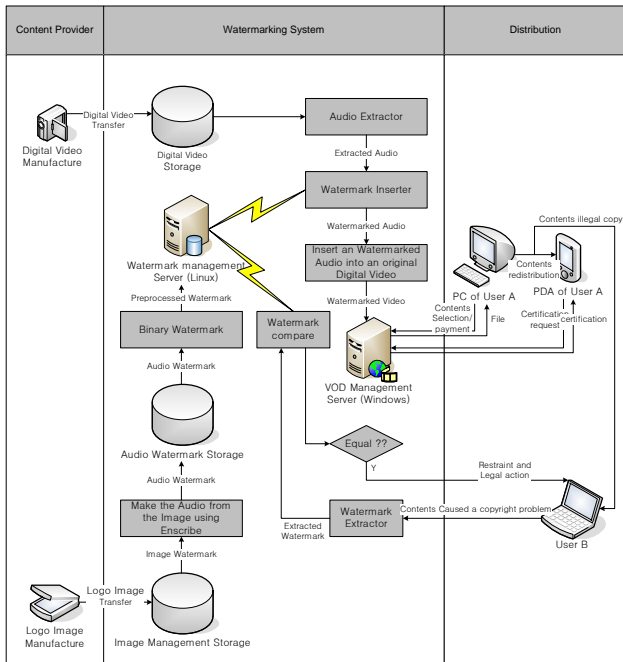


Fig 1. Proposed Digital Watermark system

Fig 1 represents the overall system of suggested model. Audio data are extracted from moving picture contents, created digital audio watermark image is inserted into audio data, to provide basis for confirmation of ownership by extracting the separate image data from audio data when copyrights and rights of possession on such digital data are demanded.

3.2 Pre-processing of watermark

Since watermark is a type of ID that represents the copyrights, it should be protected at all circumstances. For original watermark, black and white image of logo is used. The reason for using black and white logo image is for easy separation per frequency range, and to apply it for both high and low frequency.

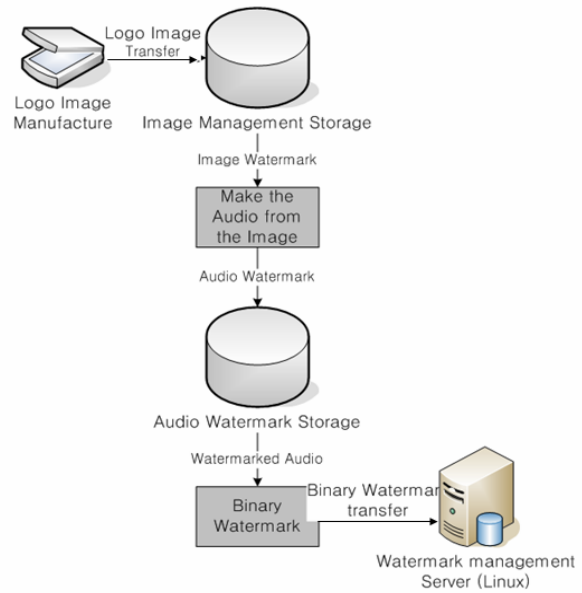


Fig 2. process of the watermark pre-processing

However, since such image has simple structure, it can be easily detected or changed, and damaged. In order to ensure security of such watermark, the following process can be taken. Scan line of original watermark image is converted into frequency range, which is then applied to IFFT (Inverse Fast Fourier Transform) and converted to audio form. Once such audio converted watermark image is produced, it can only be viewed through the 3rd frequency compression vs. time compression display. Converted watermark is saved as audio file format (.wav), and in order to insert it into digital contents, it must go through binary conversion process. Once the above procedures are completed and pre-processing of watermark is finished, the final watermark is saved in control server as shown in the Fig 2.

3.3 Insertion of watermark

In this study, in order to insert watermark to digital video composed of image (group of frames) and audio data, method inserting watermark to audio data was used, instead of inserting watermark to frame. In order to achieve this, the following steps must be taken. In order to insert watermark on audio data of digital video, audio data must be extracted first from the moving pictures. Extracted audio data must be converted to frequency range using FFT (Fast Fourier Transform), and then transformed watermark should be inserted. In order to insert watermark, one must log into control server where pre-processed watermark is saved, and select the watermark in order to increase security.

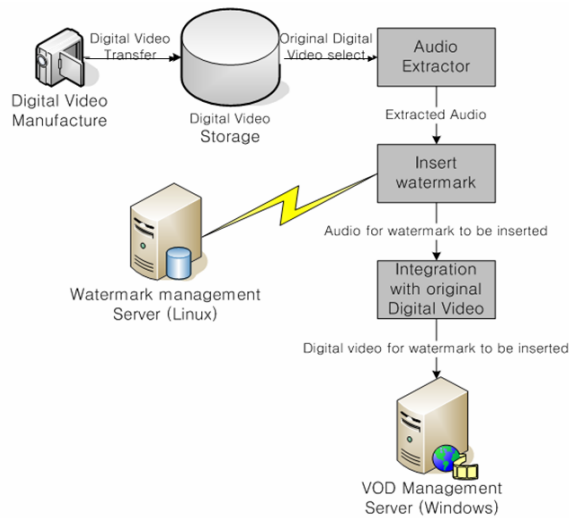


Fig 3. Watermark insertion procedure

Transformed watermark is inserted in scattered manner in proportion to time, and after inserting IFFT (Inverse Fast Fourier Transform) is used to reverse the audio data back into original signal. As the above procedures are finished and audio with inserted watermark is produced, audio data with watermark and image data are combined to create digital video with inserted watermark. Finished digital video is saved and managed at VOD control server.

3.4 Verification of ownership

If a problem related to ownership occurs, the digital video in question should be obtained and watermark extraction comparison method should be conducted to verify the correct ownership.

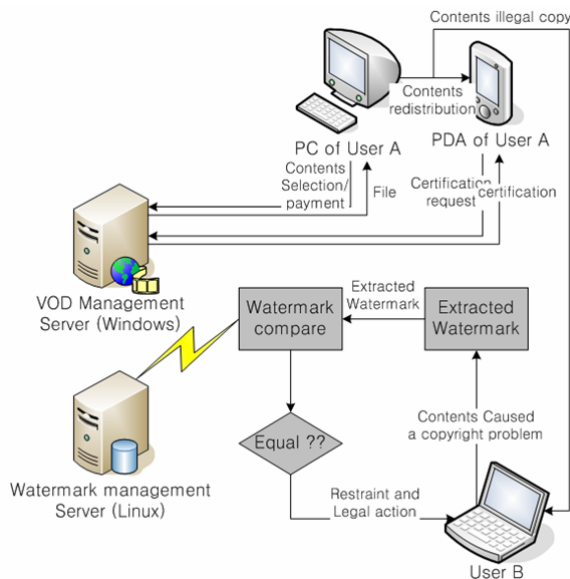


Fig 3. Ownership verification procedure

In similar manner with insertion, in order to extract the watermark audio data should be separated from digital video to identify the watermark. One must log into watermark control server, and compare the extracted watermark with original watermark, and once level of similarity above threshold value is detected, extracted watermark can be reversed to create the image of watermark, for verification of actual ownership. Once ownership is verified, sanction on illegal usage of digital content as shown in Fig 3, can be exercised.

4 Creating environment and evaluation

4.1 Creating environment

For VOD management server based on Microsoft Windows, hardware specifications with CPU 2.4GHz, RAM 1GB and Windows 2000 Server, MS-SQL Server 2000 were used. For Linux based watermark control server, hardware specifications with CPU 2GHz, RAM 512MB and Debian Linux Sarge, MySQL 4.1 database were used. For client testing, ordinary Windows and existing PC and Handheld PC, PDA etc were used, for Video control MPEG4 was used. For language on pre-processing of water-mark, Linux medium C language, and for watermark insertion development language, Microsoft Visual C++ 6.0 was used copyrights and rights of possession on such digital data are demanded.

4.2 Suggested system and test result

In the suggested system, moving picture's characteristic of being made up of image and audio data were adapted, and using the fact that for images specific characteristics exist for specific colors was used to apply it in audio frequency per frequency range.

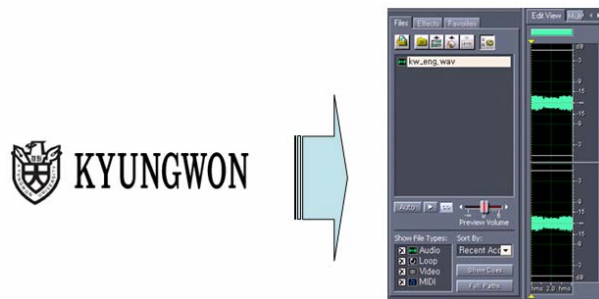


Fig 5. Digital audio conversion procedure of an image

Fig 5 shows image conversion of image data into digital audio file using suggested system. Based on brightness and darkness of the image, high frequency and low frequency data were used, and audio area was dealt with to convert image data into specific audio data.

Fig 6 shows play result of digital audio watermark image per frequency range, using windows media player,

and successful extraction of “KyungWon University” logo image from audio data, using suggested system. Of course, because low and high frequency was separated based on difference of black and white, if strong editing is done on the audio file, it will produce slight distortion.

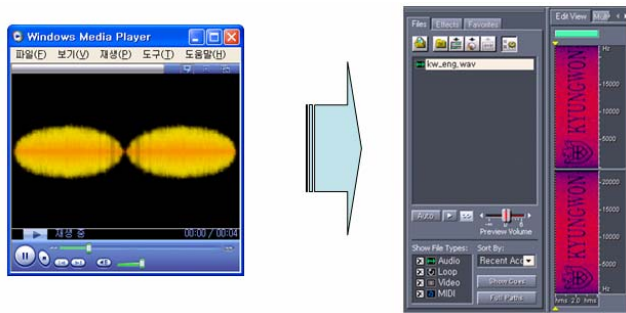


Fig 6. Audio data extraction procedure

4.3 Function evaluation

As a method to insert watermark in digital video, insertion of watermark in frame itself were commonly used, however such method produced damages to the image and from the image where tamper trials were attempted watermark could not be extracted clearly. However, in the suggested model, watermark was inserted not into the frame, but into audio data which did not degrade the quality of the image, and by using area of high and low frequency a person’s auditory area was adjusted to have no effect on audio data. Also, by passing through various steps of pre-processing on watermark, it became hard to detect. Also security of watermark it self, which represents ownership rights, was increased and different server suitable for each functions were provided in order to increase user management ability and VOD server content, which could intensify security and management.

5 Conclusion and further study

In current digital watermarking technique, it does not take into consideration the various terminal system of user, and various networks “ubiquitous computing environment” used by the user, and only reaches technique protecting distributed contents on simple Open Network alone. Also, for cases where individuals record media contents themselves, or create moving pictures, or extract moving pictures from DVD and distribute it, limiting technical copyrights and protecting such rights are very difficult. In this study, watermark was inserted to audio data, unlike insertion of watermark into video frame, to emphasize on increased security. Also, pre-processing of watermark together with managing separate server for watermark was done to increase security of ownership and copyright. Further studies on stronger and inaudible audio watermarking technique need to be done. Through new algorithm research, system that not only can be adapted to

digital video industry, but also to digital audio industry can be created and applied. Through such development, content providers can ensure legal and safe usage of contents with protected copyrights for increased reliability of users, and by preventing illegal copy and distribution of digital contents, the providers can charge users for content services for increased profit, with which the company can provide better and more unique services to the users.

6 References

- [1] S. Seneff, "Real Time Harmonic Pitch Detection," IEEE Trans. Acoust. Speech, and Signal Processing, Vol. ASSP-26, pp. 358-365, Aug. 1978.
- [2] Brandenburg K, Stoll G, “IOS-MPEG-1 Audio; A Generic Standard for Coding of High Quality Digital Audio, Journal of the Audio Engineering Society,” No.10, pp.780-792, Oct. 1994.
- [3] L.Boney, A.H.Tewfik, K.N.Hamdy, “Digital Watermarks for Audio Signals,” Proc. IEEE int.Conf. on Multimedia Computing and Systems, Hiroshima, Japan, pp.473-480, June 17-23, 1996.
- [4] M. M. Yeung and F. Mintzer, “An Invisible Watermarking Technique for Image Verifica-tion”, Proceedings of IEEE ICIP’97, Santa Barbara, CA, Oct. 1997.
- [5] M.Swanson st al, “Robust Audio Watermarking using Perceptual Masking,” Signal Process-ing, Vol. 66, No.3 , pp.337-355, May 1998.
- [6] C.Neubauer, J.Hesse, K.Brandenburg, “Continuous Steganographic Data Transmission Using Uncompressed Audio”, IHW’98 – Proc. Of the International hiding Workshop, April, 1998.
- [7] Jack Lacy, Schuyler R.Quackenbush, Amy R.Reibman and James H.Snyder, “Intellectual property protection system and digital watermarking,” OPTICS EXPRESS, Vol.3, No.12, 7. Dec. 1998.
- [8] F.Hartung and M.Kuter, “Multimedia Watermarking Techniques,” Proc. Of the IEEE, vol.87, No.7, pp.1079-1107, July 1999.
- [9] P. W. Wong and N. Memon, “Secret and public key image watermarking schemes for image authentication and ownership verification”, IEEE Trans.
- [10] F. Hartung, M. Kutter, “Multimedia Watermarking Techniques”, Proc. of IEEE, pp.1079-1107, July, 1999.

- [11] M.Swanson, B.Zhu and A.Tewfix, "Current state of the art, challenges and future directions for audio watermarking," 1999.
- [12] Changsheng Xu, Jiankang Wu, Qibin Sun and Kai xin, "Applications of Digital Water-marking Technology in Audio Signals," J.Audio eng. Soc, Vol.47, No.10, 1999.
- [13] I. J. Cox, M. L. Miller and J. A. Bloom, "Digital Watermarking", Morgan Kaufmann Pub-lishers, 2001.
- [14] J.W.Seok, J.W.Hong, "Audio watermarking for copyright protection of digital audio data," Electronics Letters, 4th, Vol.31, No.1, January 2001.
- [15] S. Jung, J. Seok, and J. Hong, "An Improved Detection Technique for Spread Spectrum Audio Watermarking with a Spectral Envelope Filter," in ETRI Journal, Vol.25, No.1, pp.52-54, February 2003.
- [16] D. Kirovski and H. Malvar, "Spread Spectrum Watermarking of Audio Signals," in IEEE Transactions on Signal Processing, Vol.51, No.4, pp.1020-1033, April 2003.