Protecting Copyright Multimedia Files by Means of Digital Watermarking: A Review

G.S. Kalra[1], ***Member IEEE***, **Dr. R. Talwar**[2], **Dr. H.Sadawarti**[2], ***Member IEEE***

[1]*Lovely Professional University, Phagwara, Punjab, India*
[2] *RIMTIET, Mandi Gobingarh, Punjab, India*

Abstract
Digital information is easy to transfer and store but this property of digital information becomes harmful to itself as it can be easily copied and distributed on the internet. Thus, number of efforts are going on to protect the copyright of the owner like Steganography, digital signatures etc. But digital watermarking comes out to be most effective tool among these. It can be applied on text, image, audio and video files in number of ways which are effective for any specific application.

Keywords: Watermarking; image; Audio; video; text watermarking.

Introduction

The growth of high speed computer networks has created new definitions for entertainment, scientific, business and social opportunities. As a result, it causes the growth of digital data. Digital media have several advantages over analog media such as high fidelity copying, easy editing, high quality etc. The digital information can be copied very easily and can be distributed easily which led to the need for effective copyright protection tools. Recent studies [1][2] show that 35% of the software programs installed in 2006 are pirated. It can be prevented if the copyright or the mark of ownership will be added in the original file in such a manner so that in case of any dispute, the actual owner can be identified. It is done by hiding data (information) within digital audio, images and video files. The ways of such data hiding is digital signature, copyright label or digital watermark that completely characterizes the person who applies it and therefore, marks it as being his intellectual property. Digital watermarking is the process that embeds data, called a watermark, into a multimedia object in such a manner that the watermark can be detected or extracted later to make a decision about the copyright of the object. The process of embedding the watermark with the secret key and detection of the watermark is shown in fig.1 (a) and fig.1 (b).The object may be an image, audio, video or text only. A simple example of a digital watermark would be a visible "seal" placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material. In addition to copyright protection, watermarking is also used in data integrity and data confidentiality. Unlike data integrity and confidentiality applications, watermarks for copyright protection applications need to be robust and invisible.

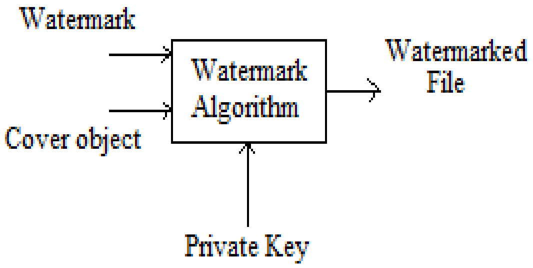

Fig.1(a): Watermark embedding process

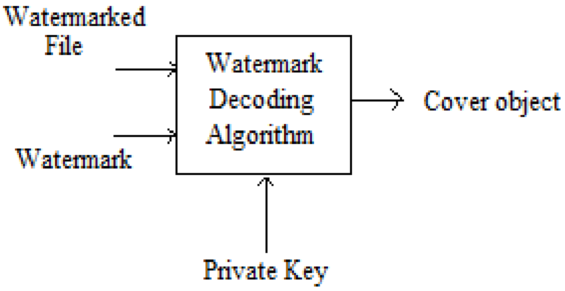

Fig.1:(b) Watermark extraction process

In general, any watermarking scheme (algorithm) consists of three parts.

- The watermark.
- The encoder (insertion algorithm).
- The decoder and comparator (verification or extraction or detection algorithm).

For a digital watermark to be effective, it should exhibit the following characteristics [3]:

1. *Adjustability.* The algorithm should be tunable to various degrees of robustness, quality, or embedding capacities to be suitable for diverse applications.
2. *Robustness.* The embedded watermarks should not be removed or eliminated by unauthorized distributors using common processing techniques, including compression, filtering, cropping, quantization and others.

3. *Security*. The watermarking procedure should rely on secret keys to ensure security, so that pirates cannot detect or remove watermarks by statistical analysis from a set of images or multimedia files. An unauthorized user, who may even know the exact watermarking algorithm, cannot detect the presence of hidden data, unless he/she has access to the secret keys that control this data embedding procedure.
4. *Imperceptibility*. The watermark should be invisible in a watermarked image/video or inaudible in watermarked digital music. Embedding this extra data must not degrade human perception about the object. Evaluation of imperceptibility is usually based on an objective measure of quality, called peak signal-to-noise ratio (PSNR) or a subjective test with specified procedures.
5. *Real-time processing.* Watermarks should be rapidly embedded into the host signals without much delay.

Watermarking Issues

There are certain issues regarding to the digital watermarking which are tried to answer ere but these are not limited to these only.

What is it?

The answer to this issue is already described above. It is a copyright mark or logo inserted in the multimedia or text file in a specific manner called algorithm so that it can be extracted only if the copyright owner wants to do it and that too if proper decoding algorithm is known exactly.

How can a digital watermark be inserted or detected?

It can be inserted and extracted with proper algorithm as shown in fig. 1(a) and fig. 1(b).

How robust does it need to be?

There are two types of watermarking as far as robustness is concerned robust and fragile. Higher robust watermark is needed if the copyright owner does not want the watermark to be extracted by himself or anyone. But fragile watermarking is also needed in those cases when authorized distribution is going to be done. The receiver receives the multimedia file along with the decoding algorithm and the key to decode the same.

Why and when are digital watermarks necessary?

When the distribution of multimedia file is done by the means of internet or by digital storage system then it can be copied and edited very easily, then watermarking becomes necessary to protect the copyright owner.

What can watermarks achieve or fail to achieve?

Watermark achieved its purpose to protect the ownership logo or copyright mark and the disputes regarding the ownership can be easily solved. But watermarking methods are not perfect against digital reformations of the file. There are different methods for different types of files (text, image, audio and video) by means of which the copyright mark can be destroyed completely or at least the mark can be destroyed in such an extent that it cannot be considered in case of any dispute.

How should digital watermarks be used?

Digital watermark must be used in a particular manner, called watermarking algorithm, which must not be a common or known method for the public. The algorithm must be kept secret. It can be extracted only with the specific decoding algorithm.

How might they be abused?

If the watermark is not embedded in a specific algorithm then the watermark can be extracted to get the original file without any copyright mark. This file can be misused and anyone can insert their watermark and can prove that this belongs to the imitator.

What are the business opportunities?

As far as business opportunities are concerned, there are two business ends which can have benefits of watermarking. One is of course the owner of the particular file and second one is the person or company which develops such method of watermarking which can be extracted without the concern of owner.

What roles can digital watermarking play in the content protection infrastructure?

The most watermarking methods developed are such that if the watermark is tried to be extracted without proper decoding algorithm, whole file gets corrupted or at least the few contents be deleted. In other words, the quality of the extracted file is much reduced.

How can we evaluate the technology?

The watermarking methods can be evaluated by certain parameters like peak signal to noise ratio (PSNR), signal to noise ratio (SNR), bit error rate (BER) or non correlation (NC).

Multimedia files and text

The watermarking technique can be applied to any text or multimedia file like image, audio or video file. The different methods of watermarking are shown in fig.2.

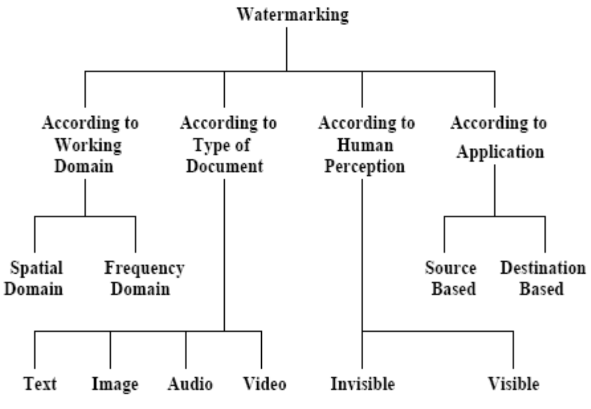

Fig.2: Watermarking methods

Watermarking techniques can be divided into four categories according to the type of document to be watermarked as follows:

- Image Watermarking [10] [11] [12]
- Video Watermarking[13] [14] [15]
- Audio Watermarking [16] [17] [18]
- Text Watermarking [19] [20] [21]

According to the human perception, the digital watermarks can be divided into two different types as follows:

- Visible watermark [22] [23]
- Invisible watermark [24] [25]

A visible watermark is a secondary image, ownership mark or a logo overlaid into the primary image. The watermark appears visible to a casual viewer on a careful inspection. The invisible-robust watermark is embedded in such a way that alternations made to the pixel value are perceptually not noticed and it can be recovered only with appropriate decoding mechanism. The invisible-fragile watermark is embedded in such a way that any manipulation or modification of the image would alter or destroy the watermark. In some cases dual watermarking is also done which means both visible and invisible watermarking is done on the same file. In this type of watermark, an invisible watermark is used as a backup for the visible watermark as clear from the fig. 3.

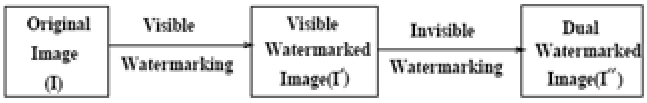

Fig. 3: Dual watermarking

According to the working domain the watermarking can be done in the spatial domain or frequency domain and according to application it can be source oriented or destination oriented.

Desired characteristics of digital watermark

The desired characteristics of digital watermark can be different depending upon the type file and type of watermarking required, that is, robust or fragile.

Desired characteristics of visible watermarks

- A visible watermark should be obvious in both color and monochrome images.
- The watermark should spread in a large or important area of the image in order to prevent its deletion by clipping.
- The watermark should be visible yet must not significantly obscure the image details beneath it.
- The watermark must be difficult to remove. Rather, removing a watermark should be more costly and labor intensive than purchasing the image from the owner.
- The watermark should be applied automatically with little human intervention and labor.

Desired Characteristics of Invisible Fragile Watermarks

- The invisible watermark should neither be noticeable to the viewer nor should degrade the quality of the content.
- An invisible fragile watermark should be readily modified when the image pixel values have been altered.
- The watermark should be secure. This means that it is impossible to recover the changes, or regenerate the watermark after image alternations, even when the watermarking procedure, and/or the watermark itself are known.
- For high quality images, the amount of individual pixel modification should be as small as possible.

Desired Characteristics of Invisible Robust Watermarks

- The invisible watermark should neither be noticeable to the viewer nor should degrade the quality of the content.
- An invisible robust watermark must be robust to common signal distortions and must be resistant to various intentional tampering solely intended to remove the watermark.
- Retrieval of watermark should unambiguously identify the owner.
- It is desirable to design a watermark whose decoder is scalable with each generation of computer.
- While watermarking high quality images and art works, the amount of pixel modification should be minimum.
- Insertion of watermark should require little human intervention or labor.

Desired Characteristics of Video and/or audio Watermarks

- The presence of watermark should not cause any visible or audible effects on the playback of the video.
- The watermark should not affect the compressibility of the digital content.
- The watermark should be detected with high degree of reliability. The probability of false detection should be extremely small.
- The watermark should be robust to various intentional and unintentional attacks.
- The detection algorithm should be implemented in circuitry with small extra cost.

Application of Digital Watermarks

Visible Watermark

Visible watermarking can be used for copyright protection for image or video files. In such cases, the content owner is in need that the images will be used commercially without payment of royalties. The content owner desires an ownership mark, that will be visually apparent, but which does not prevent image being used for other purposes. In this case, images are made available through the internet and the content owner desires to indicate the ownership of the underlying materials.

Invisible Robust Watermark

Invisible watermarking is used to detect misappropriated images. In this case, fee-generating images may be purchased by an individual who will make them available for free. Invisible watermarking can be used as evidence of ownership. In this case, the seller of the digital images suspects that one of his images has been edited and published without payment of royalties. Here, the detection of the seller's watermark in the image is intended to serve as evidence that the published image is property of seller.

Invisible Fragile Watermarks

Invisible watermarking can be used for a trustworthy camera. In this case, images are captured with a digital camera for later use in the news articles. Here, it is the desire of a news agency to verify that an image is true to the original capture and has not been edited. In this case, an invisible watermark is embedded at capture time, its presence at the time of publication is intended to indicate that the image has not been amended since it was captured. Invisible watermarking can be used to detect alternation of images stored in a digital library. The content owner desires the ability to detect any alternation of the images, without the need to compare the images to the scanned materials.

Performance evaluation of watermarking methods

The performance of any watermarking technique can be measured in any one of the parameters like BER [26], PSNR [27], SNR [28] or Non correlation [29]. They can be calculated as:

$$BER = \frac{100}{B}\sum_{n=0}^{B-1}\begin{cases}1, & \tilde{w}(n) \neq w(n)\\ 0, & \tilde{w}(n) = w(n)\end{cases}$$

Where B is the number of blocks, which is total number of bits divided by number of samples (bits) in each block, w(n) is watermark and ῶ(n) is the extracted watermark.

PSNR = 10 ——

Where,

————

X_1 and X_2 are the original audio sample and watermarked audio sample. 'R' is 255 as data type used is 8-bit unsigned number representation. If the data type is double precision floating type then 'R' will be 1.

Signal to noise ratio can be calculated as

$$SNR = 10 \cdot \log_{10}\left\{\frac{\sum_{n=0}^{N-1} x^2(n)}{\sum_{n=0}^{N-1}[\tilde{x}(n) - x(n)]^2}\right\}$$

Where *x(n)* is the original audio signal and *x (n)* as the watermarked audio signals and the normalized correlation (NC) is used to evaluate the similarity measurement of extracted binary watermark which can be calculated as

$$NC(W, W^*) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{M} W(i,j)W^*(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{M} W(i,j)^2}\ \sqrt{\sum_{i=1}^{M}\sum_{j=1}^{M} W^*(i,j)^2}}$$

Where W and W^* are original and extracted watermarks respectively, i and j are indexes of the binary watermark image.

Attacks on Watermarks

A watermarked image is likely to be subjected to certain manipulations, some intentional such as compression and transmission noise and some intentional such as cropping, filtering, etc. They are summarized in Fig.4.

Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data. Geometric distortions are specific to images videos and include such operations as rotation, translation, scaling and cropping. Common Signal Processing Operations include the following.

- D/A conversion
- A/D conversion
- Re-sampling
- Re-quantization
- Dithering distortion
- Recompression
- Linear filtering such as high pass and low pass filtering
- Non-linear filtering such as median filtering
- Colour reduction
- Addition of a constant offset to the pixel values
- Addition of Gaussian and Non Gaussian noise
- Exchange of pixels

Some other possible attacks can be as follows:

- Printing and Rescanning
- Watermarking of watermarked image (re-watermarking)
- Collusion: A number of authorized recipients of the image should not be able to come together (collude) and like the differently watermarked copies to generate an un-watermarked copy of the image.
- Forgery: A number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.
- IBM attack [7] [8]: It should not be possible to produce a fake original that also performs as well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.
- The Unzign and Stir mark have shown remarkable success in removing data embedded by commercially available programs.

Conclusions

In this paper a clear overview on watermarking concept is provided. The types of watermarking technique, whichever is required according to the application, can be applied. Further, the algorithm developed to embed the watermark can be evaluated b means of anyone of the parameters BER, PSNR, SNR and NC and at last the embedding algorithm can also be checked that weather the watermark can be survived after the attack or not.

Lossy Compression	Geometrical Distortions	Common Signal Processing Operations	Other Intentional Tampering
JPEG	Rotation	D/A or A/D conversion	Printing
MPEG	Translation	Re-sampling	Rescanning
	Scaling	Re-quantization	Rewatermarking
	Cropping	Dithering	Collusion
		compression	Forgery
		Linear filtering	IBM attack
		Non linear filtering	Unzign attack
		Colour reduction	Stirmark attack
		Addition of offset value	
		Addition of noise	
		Exchange of pixels	

Fig. 4: Possible attacks on watermarked file

References

[1] Business Software Alliances, *Piracy study, Fourth Annual BSA And IDC Global Software, 2007*, http://www.bsa.org/globalstudy/ .

[2] Industrial Design and Construction (IDC) and Business Software Alliance (BSA), *"Piracy study," July 2004.* http://www.bsaa.com.au/downloads/PiracyStudy070704.pdf

[3] Wen-Nung Lieand Li-Chun Chang, "Robust and High-Quality Time-Domain Audio Watermarking Based on Low-Frequency Amplitude Modification", *IEEE Transactions On Multimedia, Vol. 8, No. 1, February 2006*, pp.46-59.

[4] S.P.Mohanty, "A Dual Watermarking Technique For Images", *Proc. 7th ACM International MultimediaConference, ACM-MM'99*, Part 2, pp. 49-51, Orlando, USA, Oct. 1999.

[5] S.P.Mohanty, "A Dual Watermarking Technique For Images", *Proc. 7th ACM International MultimediaConference, ACM-MM'99*, Part 2, pp. 49-51, Orlando, USA, Oct. 1999.

[6] Saraju P. Mohanty, *Dept of Comp Sc and Eng, Unversity of South Florida*, Tampa, FL 33620.

[7] S.Craver, and alliance, "Can Invisible Watermarks Resolve Rightful Ownership?", *IBM Research Report, RC205209*, July25 1996.

[8] S. Craver and alliance, "Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications", *IEEE Journal. on Selected Areasin Communications*, Vol.16, No.4, May 1998, pp.573-586.

[9] Paraskevi Bassia, Ioannis Pita, and Nikos Nikolaidis, "Robust Audio Watermarking in the Time Domain", *IEEE Transactions On Multimedia*, Vol. 3, No. 2, June 2001, pp.-232-241.

[10] Myung-Ho Lee and Oh-Jin Kwon, "Color Image Watermarking Based on DS-CDMA Using Hadamard Kernel", *ICACT 2008*, Feb. 2008, pp.1592-1597.

[11] Lihong Ma and Hanqing Lu, "Adaptive Spread-transform Dither Modulation for Color Image Watermarking", *IEEE "GLOBECOM" 2008 proceedings*.

[12] A. AI-Gindya, H. AI-Ahmad, R. Qahwaji and A. Tawfik, "A Novel Blind Image Watermarking Technique for Colour RGB Images in the DCT Domain Using Green Channel", *MIC-CCA 2008*, pp.26-31.

[13] Noorkami, M. Mersereau and R.M., "Digital Video Watermarking in P-Frames With Controlled Video Bit-Rate Increase", *IEEE Transactions on information Forensics and Security, Sept. 2008*, pp 441-455.

[14] Honq-Mei Liu, Ji-Wu Huang and Zi Mei Xiao, "AN ADAPTIVE VIDEO WATERMARKING ALGORITHM", *2001 IEEE International Conference on Multimedia and Expo (ICME'01)*, August 2001.

[15] Brunton, A. Jiying Zhao , "Real-time video watermarking on programmable graphics hardware", *Canadian Conference on Electrical and Computer Engineering 2005*, May 2005, pp. 1312-1315.

[16] Xiangyang Wang, Wei Qi and Panpan Niu, "A New Adaptive Digital Audio Watermarking Based on Support Vector Regression", *IEEE Transactions On Audio, Speech, And Language Processing*, Vol. 15, No. 8, November 2007, pp. 2270-2277.

[17] Paraskevi Bassia, Ioannis Pita, and Nikos Nikolaidis, "Robust Audio Watermarking in the Time Domain", *IEEE Transactions On Multimedia, Vol. 3, No. 2, June 2001*, pp.-232-241.

[18] Lin Kezheng, Fan Bo and Yang Wei, "Robust Audio Watermarking Scheme Based on Wavelet Transforming Stable Feature", *2008 International Conference on Computational Intelligence and Security*, pp.-325-329.

[19] Xinmin Zhou, Weidong Zhao, Zhicheng Wang and Li Pan, "Security Theory and Attack Analysis for Text Watermarking", *International Conference on E-Business and Information System Security, EBISS '09*, May 2009, pp. 1-6.

[20] Hongtao Ge, Fulin Su and Yong Zhu, "**Color image text watermarking using wavelet transform and error-correcting code", 6th***International Conference on Signal Processing*, August 2002, pp.1584-1587.

[21] Qadir and Ahmad, "**Digital text watermarking:**

secure content delivery and data hiding in digital documents", *International Carnahan Conference on Security Technology, CCST '05*, Oct.2005, pp.101-104.

[22] Shang-Chih Chuang, Chun-Hsiang Huang and Ja-Ling Wu, "UNSEEN VISIBLE WATERMARKING", *ICIP 2007*, pp.III_261-III_264.

[23] Shu-Kei Yip, Oscar C. Au, Chi-Wang Ho and Hoi-Ming Wong, "Lossless Visible Watermarking", *ICME 2006*, pp.853-856.

[24] Na Li, Xiaoshi Zheng, Yanling Zhao, Huimin Wu and Shifeng Li, "Robust Algorithm of Digital Image Watermarking Based on Discrete Wavelet Transform", *International Symposium on Electronic Commerce and Security*, 2008, pp.942-945.

[25] Dumitru Dan Burdescu, Liana Stanescu, Anca Ion and Razvan Tanasie, "A NEW 3D WATERMARKING ALGORITHM*", 3DTV-CON'08*, May 2008, pp.381-384.

[26] Guo ZhiChuan and Wang JinLin Ni Hong, "A low complexity reversible data hiding method based on modulus function", *ICSP2008 Proceedings*, pp.2221-2224.

[27] Li Jing and Fenli Liu, "Applying General Regression Neural Network in Digital Image Watermarking", *Fourth International Conference on Natural Computation 2008*, pp.452-456.

[28] J. D. Gordy and L. T. Bruton, "Performance Evaluation of Digital Audio Watermarking Algorithms", *Proceedings of43rd IEEE Midwest Symposium on Circuits and Systems, Lansing MI*, Aug. 2000, pp.456-459.

[29] Chu-Hsing Lin, Jung-Chun Liu and Pei-Chen Han, "On the Security of the Full-Band Image Watermark for Copyright Protection", *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp.74-80.