

Audio Watermarking By Using Reversible Contrast Mapping (RCM)

Pandit Madhurima Rajendra¹, Swati Patil²

Department of Computer Science & Engineering¹

Assistant Professor, G.H. Rasoni Institute of Engineering and Management, Jalgaon, India²

Abstract: In recent times, communication through the internet has tremendously facilitated the distribution of multimedia data. Although this is indubitably a boon, one of its repercussions is that it has also given impetus to the notorious issue of online music piracy. Unethical attempts can also be made to deliberately alter such copyrighted data and thus, misuse it. Copyright violation by means of unauthorized distribution, as well as unauthorized tampering of copyrighted audio data is an important technological and research issue. Audio watermarking has been proposed as a solution to tackle this issue. The main purpose of audio watermarking is to protect against possible threats to the audio data and in case of copyright violation or unauthorized tampering, authenticity of such data can be disputed by virtue of audio watermarking. For this I propose a Reversible Contrast Mapping (RCM) which is a simple integer transform that applies to pairs of pixels. For some pairs of pixels, RCM is invertible, even if the least significant bits (LSBs) of the transformed pixels are lost. The data space occupied by the LSBs is suitable for data hiding.

Keywords: Reversible Contrast Mapping (RCM), least significant bits (LSBs), audio watermarking.

I. INTRODUCTION

The past few years have seen an explosion in the use of digital media. Industry is making significant investments to deliver digital audio, image, and video information to consumers and customers. A new infrastructure of digital audio, image, and video recorders and players, on-line services, and electronic commerce is rapidly being deployed. At the same time, major corporations are converting their audio, image, and video archives to an electronic form.

Along with the rapid growth of Internet, the distribution of audio visual media becomes easier. It leads to the problems regarding copyright protection. Among them, copyright protection is the primary concern and the hotspot of international area in recent areas. The embedded data are perceptually inaudible or invisible to maintain the quality of the source data. The embedded data can add features to the host multimedia signal, e.g., multilingual soundtracks in a movie, or provide copyright protection Digital product information hiding and digital watermarking technology is generated on this basis and developed along with the protection of copyright; this technology is widely used in protecting the copyright of image, audio and video by means of extracting or detecting the watermark for its various application including copyright protection, broadcast and publication monitoring, authentication, copy control.

A. Audio Watermarking

Digital audio watermarking involves the obscuring of data inside a digital audio file. Demands for this vision are numerous. Intellectual property protection is presently the main steering manipulation behind security in this area. To combat online music piracy, a digital watermark could be added to all recording prior to a discharge, signifying not merely the author of the work, but the user who has

bought a legitimate copy. The DRM multimedia will safeguard that the user has paid for the song by contrasting the watermark to the tolerating bought licenses on the arrangement.

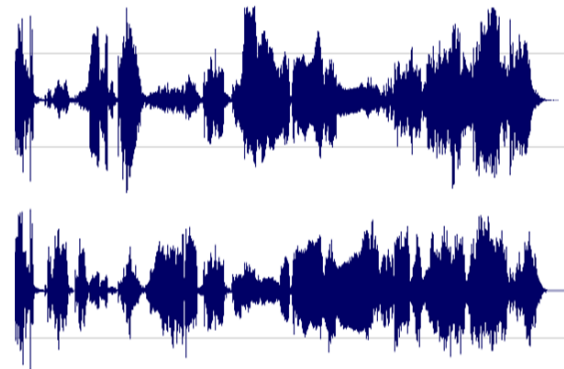


Fig.1 an Example of Digital Audio Watermark

B. Background of RCM

It introduces a new concept of compression with a different approach on lossless image compression that has been commonly known. The concept uses Reversible Contrast Mapping (RCM) which is a function of a simple integer transform developed for reversible watermarking method. The use of RCM in image compression is done similarly with the watermarking method. In this method, an image is divided into fixed-size blocks, the blocks are divided into two groups based on the data storage capacity. Blocks with smaller storage capacities are used as watermarks for the other blocks. The compression ratio of this method is similar to the Huffman compression. This method can also be used together with the Huffman compression technique to increase the overall compression ratio.

The rapid developments in information technology lead to shifting towards paperless working environment. The flow of information in a transaction does not involve physical documents but through the data files that are transmitted over a local network or the Internet. Data communication that occurs does not only transfer text documents but also involves multimedia data such as images, sound or video.

In general, the process of lossless image compression is shown in Figure 2 In contrast to the previous researches of lossless image compression methods that aim to optimize the redundancy of pixel values in the image, my project work will use watermarking techniques in the process, that store a part of the data into another part. This concept will use a simple integer transform function called Reversible Contrast Mapping (RCM).

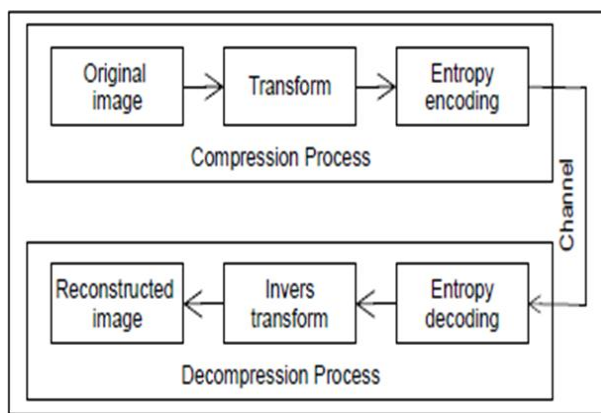


Fig.2. Lossless image compression technique

II. LITERATURE SURVEY

Traditionally, cryptography has been the principle technique for obscuring information. From the pre-computer era, encrypted messages have been exchanged between people in situations where the sender wants to ensure that the message in question cannot be understood by anyone other than those with the decrypting key. A famous example of this was the German Enigma Machine from the second world war, whose story it told in Enigma [4].

This was a machine used by the Germans with a complicated encryption technique that was eventually broken by the allied forces. As discussed previously, the rise of peer-to-peer (P2P) software has caused a surge in the ease of piracy, as discussed in Sonic Boom: Napster, P2P and the Battle for the Future of Music [2]. Piracy has always been a matter the music industry has taken very seriously but in recent years, the ease of file sharing has caused actual media sales to decline noticeably.

Since watermark is of no importance in the creation of the mark, the name is probably given because the marks resemble the effects of water on paper. Watermarking is an important mechanism applied to physical objects like bills, papers, garment labels, product packing. Physical objects can be watermarked using special dyes and inks or during paper manufacturing.

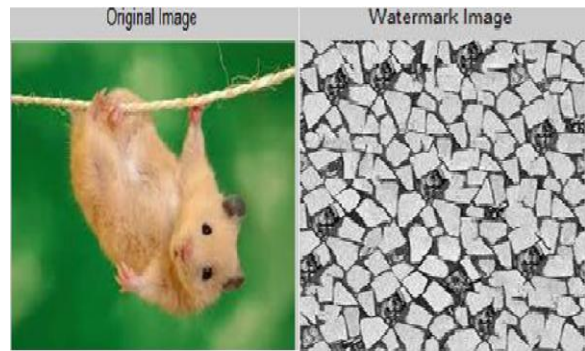


Fig. 3 Image Watermarking

It is emerging field in computer science, cryptography, signal processing & communication [2]. Watermark: is a “secret message” that is embedded into a “cover message”. Digital watermark: is a visible or perfectly invisible, identification code that is permanently embedded in the data and remains present within the data after any decryption process.

A. Digital Watermarking techniques

These are mainly as follows:-

A. Text-based Watermarking

This uses Line shift coding, word shift coding, feature coding.

B. Image Watermarking:-These are mainly

- Watermark design (meaningful watermark)
- Watermark embedding(time domain, transformed domain)
- Watermark detection(blind, informed)

C. Audio Watermarking

D. Video Watermarking

E. 3D Watermarking

B. Image Watermarking techniques

a. Spatial-domain techniques: - These are of two categories

- Least-Significant Bit (LSB) technique: The given image contains pixels these pixels are indicated by the 8-bit sequence, the watermarks are linked two the last, bit of selected pixels of the original image, it’s used to hide the information and attackers could not destroy the information.
- SSM-Modulation-Based Technique: These techniques are applied in the water marking algorithms with linked information and attached to the original image with pseudo noise.

b. Transform-domain techniques:-

These are mainly

- DCT-based
- DFT-based
- Wavelet-based
- Other transforms

c. Compressed stream-domain techniques

- Watermarking MPEG bit streams

- d. Spatial-domain watermarks
- Transparent mark
 - Visually pleasing, not robust to compression
 - Transform-domain watermarks
 - Watermark added to frequency coefficients
 - Watermark location and strength based on perceptual rules

III. IMAGE VS. AUDIO WATERMARKING

Image watermarking cannot be directly transferred to audio watermarking due to the fundamental differences between the way our eyes and ears work, as discussed in Sensation and Perception [8]. When the eye views an imperfect picture, the brain blanks out the imperfections seeing the picture as it's supposed to be viewed. For example, when a person visits the cinema, they see the projected image on the screen as it was intended to be seen without noticing the flickers unless they explicitly look out for them, but the ear can pick up on the slightest imperfection in a sound, as shown in Attacks on Copyright Marking Systems [9] When represented in visual form, it is easy to see the difference between the diagrams, just as it would be easy to tell the difference between their sounds. Here, it is evident that (b) is the same sound wave as (a) but with a 20 milliseconds echo added as a watermark.

The echo is very clearly visible at 0.02 seconds and would be easily audible when listening. The small imperfection on the picture's equivalent in the audio domain would come across as a click. A similar form of defense used in image watermarking would have been near invisible to the human eye. Despite the added complexity of audio watermarking, the similarities between the robustness techniques and the attacks of visual watermarks and audible watermarks have to be analyzed for their similarities since there is so much more literature for image watermarking and grouped as:

- Cropping (Essentially the same)
- Compression (loss or lossless)
- Random bending (pitch shifting)
- Gaussian Filtering (low-pass filter) etc.

IV. APPLICATIONS

The technique "Digital Watermarking" is the recent research in the field of multimedia and internet copyright protection field. There are various applications of DWM as broadcast monitoring, owner identification, proof of ownership, transaction hacking, content authentication, copy control, device control and so on. Out of these, some important applications are described as-

1. Broadcast monitoring: This application identifies that when and where works are broadcast by recognizing watermarks embedded in these works. There is variety of technologies to monitor playback of sound recording on broadcast. The DWM is alternative to these technologies due to its reliable automated detection. A single PC based monitoring station can continuously monitor to 16 channels over 24 hours with no human interaction.

Resulted monitoring is assembled at central server and is now available to interested one. The system can distinguish between identical versions of songs, which are watermarked for different distribution channel. Such system requires Monitoring infrastructure and watermarks to be present in content. Watermarking video or music is planned by all major entertainment companies possessing closed networks.

2. Encoding: According to the thinking of major music companies and major video studios, encoding happens at mastering level of sound recording. In such downstream, transactional watermarks are also considered. Each song is assigned with unique ID from the identifier database. After completion of all mastering processes, ID is encoded in sound recording. To enhance encoding of audio or video recordings requiring special processing, the human assisted watermark key is available.

3. Copy and playback control: The data carried out by watermark may contain information about copy and display permissions. We can add a secure module into copy or playback equipment to automatically extract the permission information and block further processing if required. This approach is being taken in Digital Video Disc (DVD).

4. Content authentication: The content authentication is nothing but embedding the signal information in Content. This signature then can be checked to verify that it has not been alter. By watermarks, digital signatures can be embedded into the work and any modification to the work can be detected.

V. CONCLUSION

The proposed method in my work is a new approach for image lossless compression. This method can be processed with a higher block size depending on the image size. Compression schema with shifting the pixel values has better compression ratio on images with an average pixels value close to the domain boundaries. The proposed method archives higher compression ratio than the Huffman compression on all the test images. The compression scheme can be used to improve the compression ratio of Huffman because it uses different compression approach. Reversible watermarking method using RCM is a variation from the basic concept of RCM function. This method can be developed using different variations of that function. In addition, another function with a specific characteristic can be implemented to this approach. Another development can be done by changing the entropy step of the commonly known lossless compression algorithms with this method.

REFERENCES

- [1] Tsung, Din-Chand. Hsieh, Ming-Shing. Huang, Yong-Huai. Hiding digital watermarks using multiresolution wavelet transform. IEEE Transactions On Industrial Electronics, 48(5):875 882, 2001.
- [2] Hwang, Min-Shiang. Chang, Chin-Chen. Hwang, Kuo-Feng. A Watermark Technique Base On One-Way Hash Functions. IEEE Transactions on Consumer Electronics, Volume 45 Issue 2. 0098-3063.

- [3] Wang, James Ze and Wiederhold, Gio. Wavemark: Digital image watermarking using daubechies' wavelets and error correction coding. In Proceedings of SPIE, volume 3528, pages 432-439, November 1998.
- [4] Z. Ni, Y.Q. Shi, N. Ansari, W. Su, Q. Sun and X. Lin, "Robust Lossless Image Data Hiding Designed for Semi-Fragile Image Authentication", IEEE Transactions on Circuits and Systems for Video Technology, vol. 18, no. 4.
- [5] J. Zhu, Q. Wei, J. Xiao and Y. Wang, "A Fragile Software Watermarking Algorithm for Content Authentication", IEEE Youth Conference on Information, Computing and Telecommunication, 2009.YC-ICT'09.
- [6] L. Robert and T. Shanmugapriya, "A Study on Digital Watermarking Techniques", International Journal of Recent Trends in Engineering, vol. 1, no. 2, (2009) May.
- [7] V. M. Potdar, S. Han and E. Change, "A Survey of Digital Image Watermarking Techniques", 2005 3rd IEEE International Conference on Industrial Informatics (INDIN).
- [8] N. Chandrakar and J. Baggaa, "Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130.
- [9] D. Mistry, "Comparison of Digital Watermarking Methods" (IJCSE) International Journal on Computer Science and Engineering, vol. 02, no. 09, (2010), pp. 2805-2909.
- [10] Hsu, Chiou-Ting and Ling, Ja. Hidden digital watermarks in images. IEEE Transactions on Image Processing, 8(1):58-68, 1999.
- [11] Oh, Hyen-O. Soek, Jong-Won. Hong, Jin-Woo. Youn, Dae-Hee. New Echo Embedding Technique for Robust and Imperceptible Audio Watermarking. International Conference on Acoustics, Speech and Signal Processing (ICASSP), Orlando, pp. 1341-1344.
- [12] Swanson, Mitchell D. Zhu, Bin. Tewfik, Ahmed H. Transparent robust image watermarking. In 1996 SPIE Conf. on Visual Communications and Image Proc., volume III, pages 211-214, 1996.
- [13] Tao, Bo. Dickinson, Bradley. Adaptive watermarking in the DCT domain. In International Conf.on Accoustics, Speech, and Signal Processing, ICASSP '97, April 1997.