IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

ANALYSIS OF DIGITAL WATERMARKING SCHEMES FOR SECURING DIGITAL MEDIA

Dilshad Ali*, Sachin Tyagi
* Scholar Master of Technology, Dept. of Electronics and Communication Engineering, Roorkee College of Engineering, Roorkee, UK, India.
Assistant Professor, Dept. of Electronics and Communication Engineering, Roorkee College of Engineering, Roorkee, UK, India.

ABSTRACT

With the proliferation of digitized media, the need of digital watermarks as a copyright protection, ownership identification and a secure way of embedding information has become important. A useful watermark technique should be robust against malicious attacks or tampering to remove the watermark and should not greatly affect the quality of the original file. Every watermarking system has two main parts: watermark embedding and watermark extraction/decoction. In conventional cryptographic systems, once the information is decrypted, the recipient can misuse it. The reproduction and retransmission cannot be tracked easily. In this dissertation thesis, selected major watermarking techniques are investigated for digital image as well as audio files. The selection was carried out after intensive study and feasibility checking of latest available techniques. The robustness and effectiveness of these watermarking techniques are tested both quantitatively and qualitatively. The results obtained after experimental study of watermarking of, digital image for LSB technique in image-image, image-text and circular watermarking technique, digital audio for Echo hiding, amplitude modulation, and high frequency modulation are more than satisfactory. The watermark has been embedded and extracted successfully without affecting the quality of original file in noticeable extent.

KEYWORDS: Digital watermarking, Cryptographic images, Echo hiding etc.

INTRODUCTION

As audio, video and other works become available in digital form, the ease with which perfect copies can be made, may lead to large-scale unauthorized copying which might undermine the music, film, book and software industries. These concerns over protecting copyright have triggered significant research to find ways to hide copyright messages and serial number into digital media. An important sub discipline of information hiding is steganography. While cryptography is about protecting the content of messages, steganography is about concealing their very existence. Watermarking, as opposed to steganography, has the additional requirement of robustness against possible attacks. The information hidden by a watermarking system is always associated to the digital object to be protected or to its owner while steganographic systems just hide any information. The robustness criteria are also different, since steganography is mainly concerned with detection of the hidden message while watermarking concerns potential removal by a pirate. Generally, steganographic communications are usually point to point (between sender and receiver) while watermarking techniques are usually one to many.

AIMS AND OBJECTIVES

The aim of this dissertation is to implement digital watermarking schemes for securing digital media. Current research in the area of image and audio watermarking is to be investigated, and the robustness of simple watermarking methods should be experimentally evaluated using a suitable software platform.

The algorithm is designed based on the watermarking proposed in the literature and coded using MATLAB software. In addition, their effectiveness will be determined when subjected to robustness of watermarking retrieval with maintaining quality of original signal.

METHODOLOGY

Research the background information relating to watermarking and other information hiding techniques. This is accomplished by researching for relevant materials from the libraries and Internet.

- Research the possible application areas of digital watermarking. After gaining knowledge of the background information relating to watermarking, the application areas are studied. This allows a better understanding on how the watermarks are used in different applications. Most of the materials are found in libraries and online materials.
- Investigate several different watermarking algorithms. The different watermarking techniques are studied before the actual designing and programming of the algorithm. The types watermarking algorithms are research from the background of information hiding techniques and digital watermarking.

INFORMATION HIDING ENCRYPTION

Encryption is the process of transforming information to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now used in protecting many kinds of civilian systems, such as the Internet e-commerce, mobile telephone networks and bank automatic teller machines. Encryption is also used in digital rights management to restrict the use of copyrighted material and in software copy protection to prevent against reverse engineering and software piracy.

Encryption, by itself, can protect the confidentially of messages, but other techniques are still needed to verify the integrity and authenticity of a message; for example, a message authentication code (MAC) or digital signatures. Standards and computer programs to perform encryption are widely available, but successfully using encryption to ensure security is a challenging problem. A single slip-up in system design or execution can allow successful attacks. And sometimes an adversary can obtain valuable information without directly undoing the encryption.

Digital watermarking

Digital Watermarking is an authentication technique which permanently embeds a digital signal (watermark) in text, image, audio, video files (any Data) by slightly modifying the data but in such a way that there are no harmful effects on the data. The watermark embedded may contain information such as identification of the product's owner, user's license information etc. This watermark can then be detected whenever required to identify its owner or to check whether a user is authentic to access that data or no.

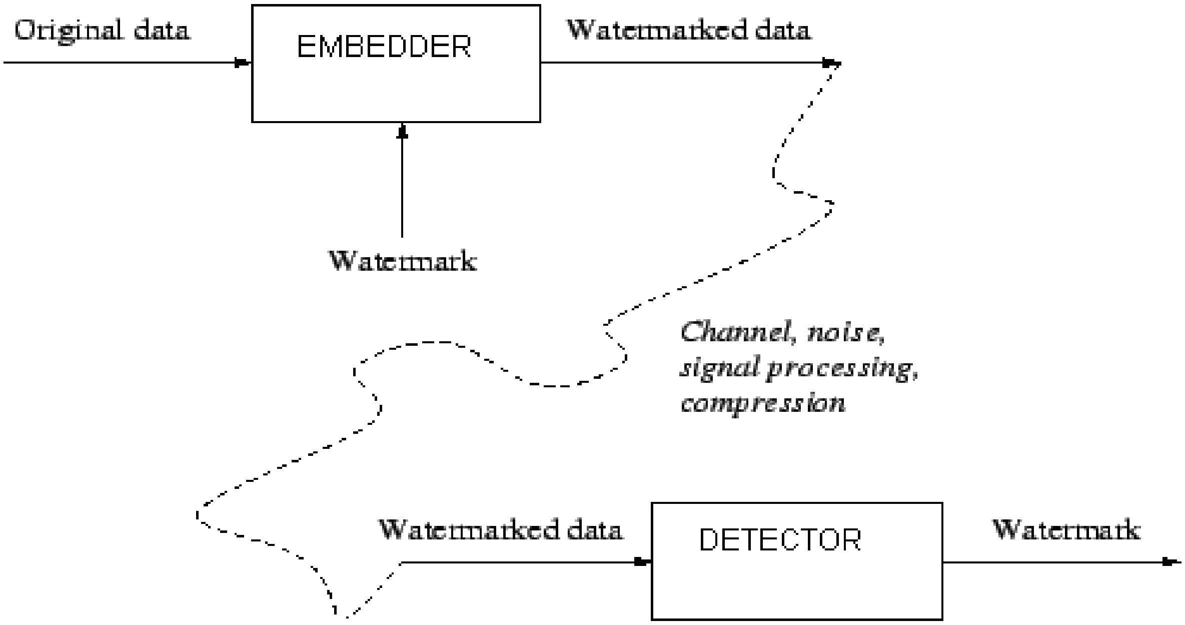


Fig. 1: A generic diagram of digital watermarking.

Basic Watermarking Principles

All watermarking methods share generic building blocks: a watermark embedding system and a watermark recovery system also called watermark extraction or watermark decoder. The input to the watermark embedding process is the watermark, the cover data and an optional public or secret key. The watermark can be of any nature such as number, text, or an image. The key may be used to enforce security that is the prevention of unauthorized parties from recovering and manipulating the watermark. All practical system employs at least one key, or even a combination of several keys. In combination with a secret or a public key the watermarking techniques are usually referred to as secret and public watermarking techniques, respectively. The output of the watermarking scheme is the watermark data.

PROPERTIES OF WATERMARKS

Digital watermarking hides data in a file by inserting a small amount of information throughout in such a way that the file can still be viewed. If the watermark is removed, the content of the media will be destroyed. When digital watermarking is applied, the purpose is to find information in the file that can be modified without having a significance impact on the actual content. Errors will be introduced into the content when a watermarked is applied. If the errors are low, the overall impact on the content will usually be minimal. To classify a good watermarking technique, there are several criteria that a good watermark for an image must fulfill. These are as follows:

Unobtrusive: A watermark is a perceptually unobtrusive signal embedded in an image, an audio or video clip, or any other multimedia asset. Its purpose is to be a label, which is attached to the content. The watermark signal should not affect or degrade the original image significantly. For the best result, the end user should not be able to distinguish any differences between the original and watermarked image by looking using their naked eye. The watermark should only be detected if the secret key is known.

Robustness: Robustness refers to the ability to detect the watermark after common signal processing. For image, it includes spatial filtering, lossy compression, printing and scanning, and geometric distortions. Video watermarks may need to be robust to the same transformation as well as recording of video, changes in frame rate. Audio watermarks may need to be robust to process such as temporal filtering, recording on audiotape and variations in playback speed. The watermark must be difficult to remove and remain in the media content after the attack.[8]

Unambiguous: Retrieval of the watermark should clearly be able to identify the owner, and the accuracy of identification should degrade gracefully in the face of attack.

Undeletable: The watermarks should be difficult to be removed by any hacker, without degrading the visual quality of the image.

Statistically Invisible: To be statistically invisible means that the attacker is unable to detect the embedded message by comparing several different watermarks from the same author. This means that the watermark should not be obtained through statistical analysis on few different sets of watermarked data.

Multiple Watermarking: The watermarking scheme should allow multiple data to be embedded into the same image for different authorized users. This data should be fully and unambiguously retrievable by the rightful owner with their corresponding use key.

RESULTS

Through this whole project we have studied thoroughly the whole field of digital watermarking and obtained a large variety of results and developed an in depth understanding about the watermarking techniques which we have tested and implemented successfully by writing matlab codes for each one of them and then testing these codes as an application suite for watermarking different digital media with different types of watermarks using all the previously mentioned and latest techniques employing improvements in already existing ones which is very clearly understood through our results. Finally this whole study puts us in a position to say very convincingly that which technique will give best possible performance in what conditions and this leads us to enable a user to finally get the most efficient and performance wise the best technique for watermarking the data available in a very user friendly and lucid way through a **GRAPHICAL USER INTERFACE** which we have developed in due course of this project.

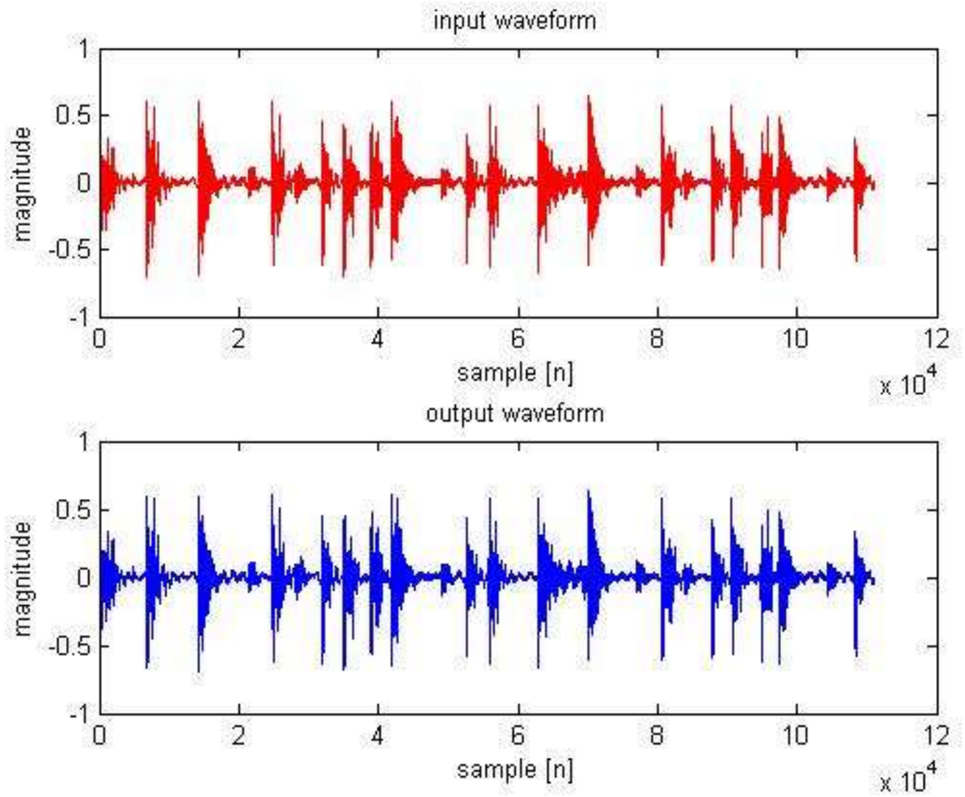


Fig. 2: Audio input-output waveform 1 for echo hiding

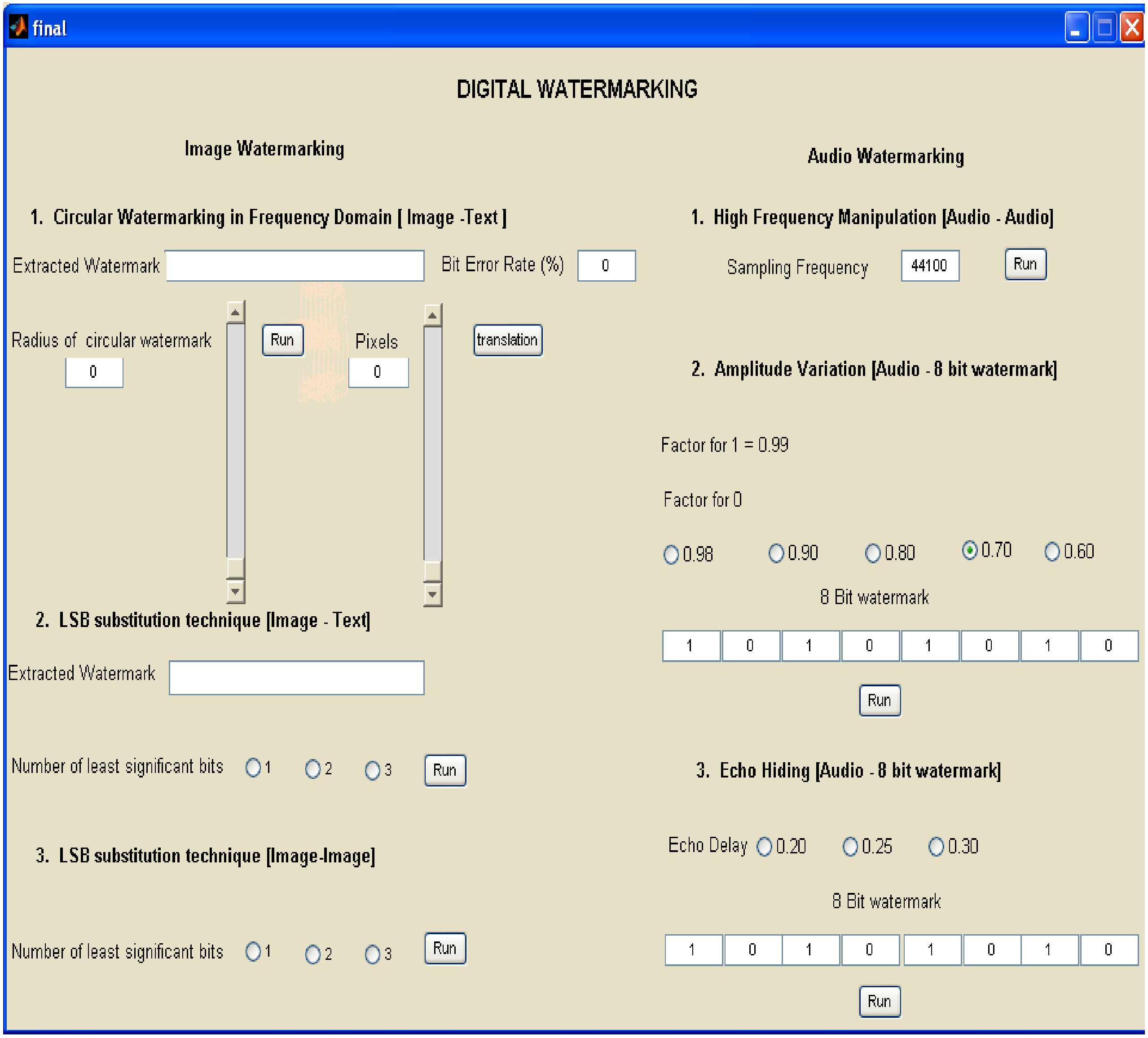
ADVANTAGES

Detection of the watermarked signal is simple and straightforward using amplitude variation technique. The variations in host file are inaudible to the human ear as change made in coefficient is very small but are consequently highly subject to additive noise. The process of embedding a watermark is spread out across blocks of the original host signal so this technique also requires knowledge of host signal. So we can say that this technique is not suitable in highly noisy environments. Most significant advantage is high immunity to resynchronization attacks.

GRAPHICAL USER INTERFACING

In this paper we have also developed an user friendly graphical user interface so as to enable a novice user to watermark different digital media comprising audio and images. The language used to write the code for this GUI is chosen as MATLAB .The main features of this GUI are the facilities for watermarking using 6 different watermarking techniques including for audio domain and for image domain. The snapshots for this GUI are shown in figures.

Fig. 3: GUI screenshot Main window



1. Circular Watermarking in Frequency Domain [Image -Text]

Extracted Watermark

Bit Error Rate (%) 0

Radius of circular watermark 0

Pixels 0

2. LSB substitution technique [Image - Text]

Extracted Watermark

Number of least significant bits ○ 1 ○ 2 ○ 3

3. LSB substitution technique [Image-Image]

Number of least significant bits ○ 1 ○ 2 ○ 3

1. High Frequency Manipulation [Audio - Audio]

Sampling Frequency 44100

2. Amplitude Variation [Audio - 8 bit watermark]

Factor for 1 = 0.99

Factor for 0

○ 0.98 ○ 0.90 ○ 0.80 ● 0.70 ○ 0.60

8 Bit watermark

1	0	1	0	1	0	1	0

3. Echo Hiding [Audio - 8 bit watermark]

Echo Delay ○ 0.20 ○ 0.25 ○ 0.30

8 Bit watermark

1	0	1	0	1	0	1	0

CONCLUSION

Digital audio watermark technology is an active research area in industry. The force currently driving development is intellectual property protection, via copy-prevention and detection systems. The digital watermark has great potential to be used as part of an overall system for managing IP rights, and can be used not only to signify the author of a particular audio file, but catalog the path a particular file takes if it is distributed in an unauthorized manner. The main advantage of the LSB watermarking technique is its high payload, whereas the main disadvantage lies in its low robustness, due to the fact that random changes destroy the coded watermark.

REFERENCES

[1] Stefan Katzenbeisser, Fabien A.P. Petitcolas, "Information Hiding: Techniques for steganography and digital watermarking", Artech House, 1999.

[2] Wen-Nung Lie, Li-Chun Chang, ”Robust and High-Quality Time-Domain Audio Watermarking Based on Low-Frequency Amplitude Modification” in IEEE Transaction on multimedia, vol. 8, no. 1, pp.48-52, February 2006

[3] Siriporn Pholsomboon and Sartid Vongpradhip, “Rotation, Scale, and translation Resilient Digital Watermark Based on Complex Exponential Function” in ECTI transactions on electric eng, Electronics and communication, vol2, no.2, pp.40-47, august 2004

[4] Ingemar J. Cox, Senior, Joe Kilian, F. Thomson Leighton, and Talal Shamoon, “Secure Spread Spectrum Watermarking for Multimedia” in IEEE Transaction on Image processing, vol. 6, no. 12, pp.1677-1682, December 1997

[5] Juan R. Hernandez Martin, Lysis SA Martin Kutter, Alpvision SARL “Information Retrieval in Digital Watermarking” in IEEE Communications Magazine, pp.110-116, August 2001

[6] Onkar Dabeer, Kenneth Sullivan, Upamanyu Madhow, Shivakumar Chandrasekaran, and B. S. Manjunath, “Detection of Hiding in the Least Significant Bit” in IEEE transaction on signal processing, vol. 52, no. 10, pp.3046-3057, October 2004

[7] Sonia Djaziri Larbi and Mériem Jaïdane-Saïdane “Audio Watermarking: A Way to Stationnarize Audio Signals” in IEEE transaction on signal processing, vol. 53, no. 2, pp.816-822, February 2005

[8] Kutter, M. (2001), Digital Watermarking Frequently Asked Questions. http://www.watermarkingworld.org/faq.html current March 2004.

[9] V. Licks and R. Jordan, “On Digital Image Watermarking Robust to Geometric Transformations,” Proceedings of 2000 International Conference Image Processing (ICIP 2000), Vol. 3, pp. 690-693. Vancouver, BC, Canada, September 10-13, 2000.