International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 7, No. 2
May 2018

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 7, No. 2, May 2018

Research Paper

DESIGN OF VIDEO IN VIDEO STEGNOGRAPHY SYSTEM USING WATERMARKING TECHNIQUES

D Pradeepa[1]* and Sountharya[2]

*Corresponding Author: D Pradeepa

Received on: 31st March, 2018 Accepted on: 15th April, 2018

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. “Watermarking” is the process of hiding digital information in a carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. This technique consists of video processing, frame extraction, histogram equalization, Least Significant Bit substitution (LSB) and frame concatenations. It provides higher security to the transmitting video.

Keywords: Stenography, Watermarking, Design of video

INTRODUCTION

Watermarking technique is used for information hiding which is used to conceal proprietary information in digital media as photographs, digital video, digital music, etc. The ease with which digital content can be exchanged over the Internet has created copyright infringement issues. Over peer to-peer networks, copyrighted material can be easily exchanged, and this makes serious concerns to those content providers who produce these digital contents. This paper provides survey of watermark techniques for files like video, text, images and audio.

REVIEW ON DIGITAL WATERMARKING

Digital watermarking is one of the best solutions to prevent illegal copying, modifying and redistributing multimedia data. Encryption of multimedia products prevents an intruder from accessing the contents without a proper decryption key. Digital watermarking is an effective solution. Copyright protection, data authentication, covert communication and content identification can be achieved by Digital watermarking. Digital watermarking is a technique to embed copyright or other information into the underlying data, the algorithm should meet few basic requirement).

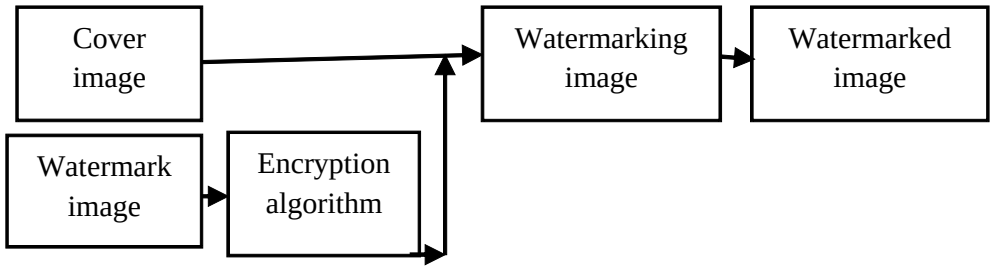
Imperceptibility: The watermark should not affect the quality of the original signal, thus it should be invisible/inaudible to human eyes/ears.

Robustness: The watermarked data should not be removed or eliminated by unauthorized

[1] ME (VLSI) Student, Star lion College of Engineering and Technology, Manangorai, Thanjavur, Tamil Nadu, India.

[2] Assistant Professor, Department of ECE, Star lion College of Engineering and Technology, Manangorai, Thanjavur, Tamil Nadu, India.

Figure 1: Process of Digital Watermarking



distributors, thus it should be robust to resist common signal processing manipulations such as filtering, compression, filtering with compression.

Capacity: The number of bits that can be embedded in one second of the host signal.

Security: The watermark should only be detected by authorized person.

Watermark detection should be done without referencing the original signals.

The watermark should be undetectable without prior knowledge of the embedded watermark sequence.

The watermark is directly embedded in the signals, not in a header of the signal.

DEFINITIONS OF DIGITAL WATERMARKING

Digital Watermarking technique [1] means the process to embed the given watermark information (Such as symbol, possessory name, signature. etc.,) into the protective information (such as sound, picture, video) and picking the given watermark information from the protective information, which is not perceived by human perceptual system (Figure 1).

Watermarking depicts the fundamental process of digital watermarking technique. it gives enough detail about watermarking requirements and its various types like fragile and robust watermarking.

CLASSIFICATION OF INFORMATION HIDING

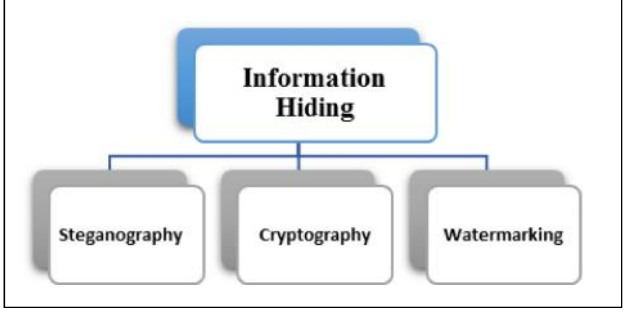
Steganography (art of hidden writing)

A term derived from the Greek words “steganos” and “graphia” (The two words mean “covered” and “writing”, respectively). The art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. The existence of information is secret.

Cryptography

The conversion of data into a secret code for transmission over a public network. Today, most cryptography is digital, and the original text (“plaintext”) is turned into a coded equivalent called “cipher text” via an encryption algorithm.

Figure 2: Classification of Information Hiding



CHARACTERISTICS OF DIGITAL WATERMARKING

Some characteristics of digital watermarking are

Invisibility: An embedded watermark is not visible.

Robustness: Piracy attack or image processing should not affect the embedded watermark.

Readability: A watermark should convey as much information as possible. A watermark should be statistically undetectable.

Security: A watermark should be secret and must be undetectable by an unauthorized user in general. This requirement is regarded as a security and the watermark is usually achieved by the use of cryptographic keys.

THREE STEPS OF WATERMARKING SYSTEM

A watermarking system is usually divided into three distinct steps

- Embedding
- Attack
- Detection/Extraction

Embedding

In embedding, an algorithm accepts the host and the data to be embedded, and produces a watermarked signal.

Inputs to the scheme are the watermark, the cover data and an optional public or secret key. The outputs are watermarked data. The key is used to enforce security.

Attacks

The watermarked digital signal is transmitted or stored, usually transmitted to another person. If this person makes a modification, this is called an *attack*.

Extraction

Extraction is an algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted.

WATERMARKING CLASSIFICATION

Digital Watermarking techniques can be classified in a number of ways depending on different parameters.

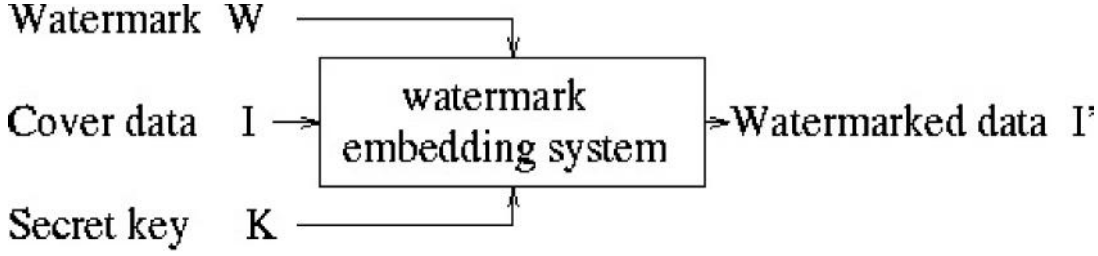
Robust and Fragile Watermarking

Robust watermarking is a technique in which modification to the watermarked content will not affect the watermark.

Visible and Transparent Watermarking

Visible watermarks are ones, which are embedded in visual content in such a way that

Figure 3: Embedding



they are visible when the content is viewed. Transparent watermarks are imperceptible and they cannot be detected by just viewing the digital content.

Public and Private Watermarking

In public watermarking, users of the content are authorized to detect the watermark while in private watermarking the users are not athorized to detect the watermark.

Asymmetric and Symmetric Watermarking

Asymmetric watermarking (also called asymmetric key watermarking) is a technique where different keys are used for embedding and detecting the watermark. In symmetric watermarking (or symmetric key watermarking) the same keys are used for embedding and detecting watermarks.

Steganographic and Non-Steganographic Watermarking

Steganographic watermarking is the technique where content users are unaware of the presence of a watermark. In nonsteganographic watermarking, the users are aware of the presence of a watermark. Steganographic watermarking is used in fingerprinting applications while nonsteganographic watermarking techniques can be used to deter piracy.

WATERMARKING TECHNIQUES

Spatial Domain Techniques

Some of the Spatial Techniques of watermarking are as follow.

Least-Significant Bit (LSB)

The earliest work of digital image watermarking schemes embeds watermarks in the LSB of the pixels. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (i.e., least significant), bit, of selected pixels of the image.

SSM-Modulation-Based Technique

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time or frequency domains.

Frequency Domain Techniques

Compared to spatial-domain methods, frequency-domain methods are more widely applied. The aim is to embed the watermarks in the spectral coefficients of the image

Discrete Cosine Transformation (DCT)

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space.

Figure 4: Block Diagram of Proposed System

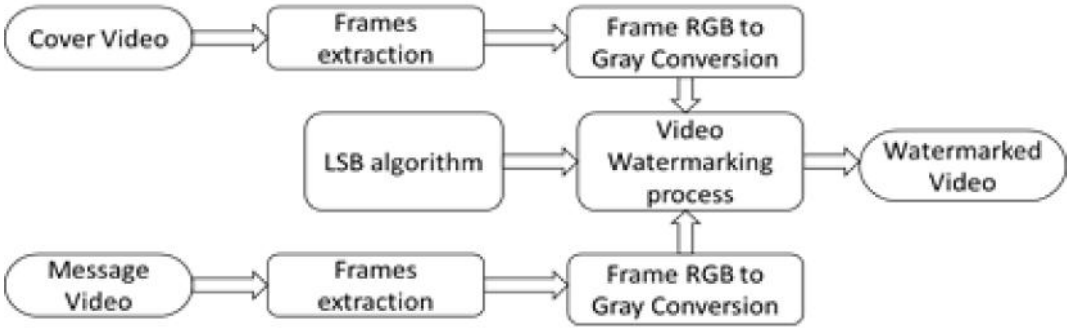
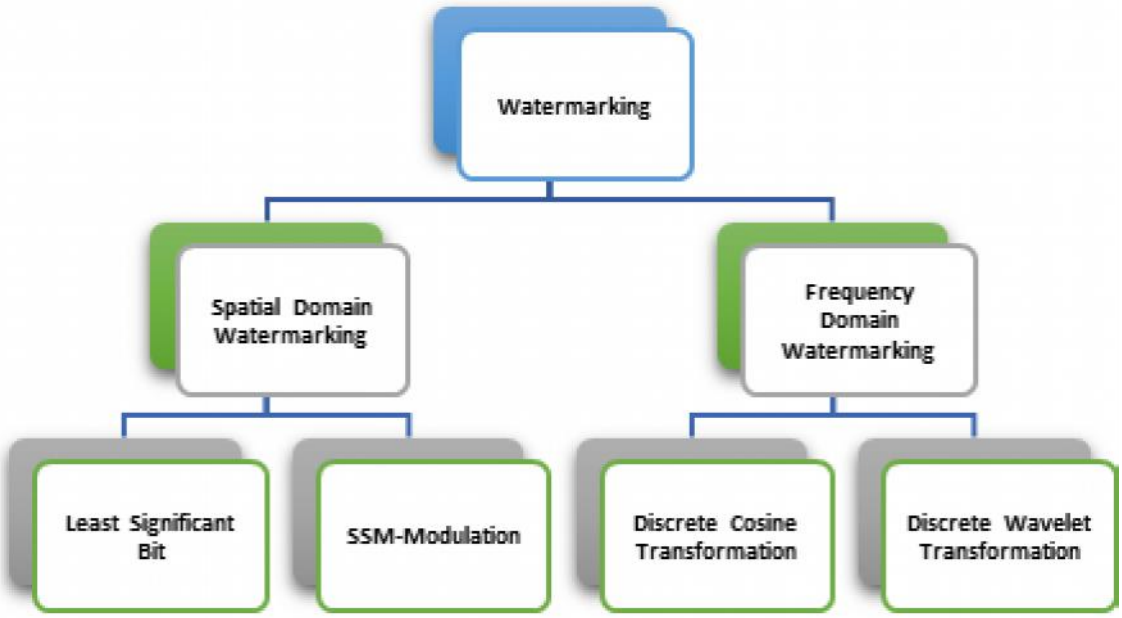


Figure 5: Block Diagram of Watermarking Techniques



Discrete Wavelet Transformation (DWT)

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals.

Backdrops of Above Mentioned Watermark Technique Systems

- Scope
- Tamper Proofing
- Inseparability
- Transparency / Visibility
- Insecurity

Fast Hadamard Transform (FHT)

FHT Technique/Algorithm has many advantages over above mentioned techniques, are:

- Shorter processing time
- Invisibility of the watermark guaranteed
- Increased watermark energy least

2D-Hadamard Transform of Signal

The 2D-Hadamard transform has been used extensively in image processing and image compression Let [*U*] represents the original image and [*V*] the transformed image, the 2D-Hadamard transform is given by:

$$[V] = \frac{H_n [U] H_n}{N}$$

where *Hn* represents an *N*×*N* Hadamard matrix, $N = 2n$, $n = 1, 2, 3, \ldots$, with element values either +1 or –1. The advantages of Hadamard transform are that the elements of the transform matrix *Hn*are simple: they are binary, real numbers and the rows or columns of *Hn*are orthogonal.

Since H_n has N orthogonal rows $H_n H_n = NI$ (I is the identity matrix) and $H_n H_n = NH_n H_n^{-1}$, thus

$H_n^{-1} = H_n/N$. The inverse2D-fast Hadamard transform (IFHT) is given as

$$[U] = H_n^{-1}[V]H_n^* = \frac{H_n[V]H_n}{N}$$

In our watermarking algorithm, the forward and reverse Hadamard transform is applied to the sub-blocks of the original or watermarked images.

For $N = 2$, the Hadamard matrix, $H1$, is called a core matrix, which is defined as

$$H_1 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

The Hadamard matrix of the order n is generated in terms of Hadamard matrix of order n-1 using Kroneckerproduct, $\otimes$, as

$H_n = H_{n-1} \otimes H_1$

Or

$$H_n = \begin{bmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & -H_{n-1} \end{bmatrix}$$

Since in our algorithm, the processing is carried out based on the 8×8 sub-blocks of the whole image, the third order Hadamard transform matrix $H3$ is used. By applying (5) or (6), $H3$ becomes:

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}$$

The characteristic of the rows or columns of $H3$ is sign transitions, which is defined as a 1 to –1 or –1 to 1 change. In $H3$, the number of transitions for row 1 to row 8 is 0, 7, 3, 4, 1, 6, 2 and 5 according to equation. The number of sign changes is referred to as sequency. The concept of sequency is analogous to its Fourier counterpart frequency. Zero sign transitions correspond to DC and a large number of sign transitions correspond to high frequency. In Hadamard matrix $H3$, the elements are not arranged in increasing sequency, such that the number of transitions is 0, 1, 2, 3, 4, 5, 6 and 7. If the order of rows is in ascending of sequency, this transform matrix is called a Walsh transform matrix. A Walsh transform may cause the transformed matrix to have DC value at upper left corner and AC coefficients arrange in Zigzag order from low frequency components to high frequency components. The Walsh transform is not used here because the middle and high frequency AC components, which could be watermarked has shown to be somewhat unreliable and the performance worse than existing DCT watermarking algorithms. On the contrary, the Hadamard transform matrix $H3$ has its AC components in Hadamard.

REFERENCES

1. Christine I Podilchuk and Edward J Delp (2001), “Digital Watermarking: Algorithms and Applications”, *IEEE Signal Processing Magazine*.
2. Cox I J, Kilian J, Leighton F T and Shamoon T (1997), “Secure Spread Spectrum Watermarking for Multimedia”, *IEEE Transactions on Image Processing.*
3. Cox I J, Miller M L and Bloom J A (2001), *Digital Watermarking*, 1st Edition.

4. Jian Liu and Xiangjian He (2005), "A Review Study on Digital Watermarking", *Information and Communication Technologies*.
5. Juergen Seitz (2005), "University of Cooperative Education Heidenheim, Germany", *Digital Watermarking for Digital Media*, 1st Edition, May.
6. Michael Arnold, Martin Schmucker and Stephen D Wolthusen (2003), "Techniques and Applications of Digital Watermarking and Content".
7. Swanson M, Zhu B, Tewfik A and Boney L (1997), "Robust Audio Watermarking Using Perceptual Masking", *Signal Process*, Special Issue on Watermarking.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com