An Improved Scheme for Digital Watermarking Based On Discrete Cosine Transformations

Ajay Goel$^{a}$, O.P.Sahu$^{a}$, Rupesh Gupta$^{c}$, Sheifali Gupta$^{c}$

Abstract - Digital Watermarking is a technology of embedding watermark with intellectual property rights into images, videos, audios and other multimedia data by a certain algorithm. The basic characteristics of digital watermark are imperceptible, security, reliability, low complexity of watermarking algorithm and security of the hiding place. Digital Watermarking Algorithm is composed of three parts: watermark embedding algorithm, the watermark extraction algorithm and the watermark detection algorithm. Future research of digital watermarking technology will focus on the watermarking algorithm, the study of watermarking theories, the watermark attacks and the evaluation system of watermarking system. A robust digital watermarking approach is proposed using the modified discrete cosine transformation (MDCT). The quality of the watermarked image is high and is robust to compression, noises, filtering and geometric transformations.

Keywords - Watermarking Techniques, robustness, DCT, Spread Spectrum Approach, Masking, MDCT, Copyright Protection.

I. INTRODUCTION

The use of digitally formatted audio, video, and printed information is increasing rapidly with the expansion of multimedia broadcasting, networked databases, electronic publishing, etc. This progressive switch to digital representation of multimedia information (text, video, and audio) provides many advantages, such as easy and inexpensive duplication and distribution of the product. However, it also increases the potential for misuse and theft of such information, and significantly increases the problems associated with enforcing copyrights on multimedia information [5],[1],[2] the protection and enforcement of intellectual property rights has become an important issue in the digital world. Well-established organizations are actively pursuing research into digital watermarking and are calling for proposals to incorporate these methods in current multimedia standards. There are various watermarking schemes applied to images and several methods applied to audio and video streams, among them; a large class of the watermarking schemes addresses invisible watermarks. We are currently in an evaluation phase of the technology in which researcher are developing general guidelines for effective watermarking algorithm design, improving reliability within the constraints of computational complexity and tailoring to the constantly changing needs of multimedia industries [5]. During the past few years, a number of digital watermarking methods have been proposed. The two basic modalities for image watermark encoding are: spatial domain techniques (spatial watermarks) and spatial frequency-domain techniques (spectral watermarks). The following paper describes spatial watermarking algorithms that rely on some type of perceptual knowledge in the encoder. Spatial watermarking techniques provide simple and effective schemes for embedding an invisible watermark into the original image but are not robust to common image alterations. Another way to mark an image is to transform it into the frequency domain- Fourier, DCT, wavelet, etc. - before marking it. The mark is incorporated directly into the transform coefficients of an image. The inverse-transform coefficients form the marked image. These types of algorithms are often called spectral watermarks, and commonly use frequency sensitivity of the human visual system to ensure that the watermark is invisible. Many of these techniques are private watermarks, which require the original image to verify the mark. Algorithms that do not require the original image for testing are called public watermarks [2]. Some modified approach are required to perk up the robustness later than the compression of images.

II. APPLICATION AREAS

1) Copyright protection: Embedding the ownership of the information when the information is being duplicated or abused.

2) Usage/Copy tracking: Verify the usage and copy of the information by the embedded data. Metadata or additional information: Embedding data to describe the information, e.g., structure, indexing terms, etc. Multiple data embedding: Embedding smaller image in a larger image or multiple audio data in a video.

3) Post-processing of watermarked data: Some watermarked data are required to undergo some lossy signal-processing operations. For examples, images for storage and transmission may perform lossy coding operation in order to reduce bit rates and increase efficiency.
III. GENERAL REQUIREMENTS

It is noted that one of the basic requirements for digital watermarking is to maintain the quality of the original data not being distorted when a watermark is embedded into it. Besides, there are other requirements that are necessary for specific applications. Perceptual transparency and robustness are the most common requirements for applications. Some other requirements, such as capability to recover data without original data, bit rate of data embedding algorithm, security, unambiguous proof of ownership, may be required for specific applications.

1. Perceptual transparency: Perceptual transparency means that the embedded watermark is undetectable perceptually. If humans cannot differentiate between the original data and the watermarked data, the watermark is imperceptible. Blind tests are usually conducted to measure the perceptual transparency, where human subjects are presented with data with or without watermark randomly and asked to determine the quality. Perceptual transparency is required for applications in copyright protection, usage tracking and embedded metadata.

2. Robustness: The watermarked data may be processed by some signal processing operations. After operations, the watermarked data is modified or manipulated, the embedded watermark may have been destroyed. The robustness of watermarking ensures that the embedded watermark will not be destroyed after such operations. As a result, third parties are not able to modify the watermarked data to thwart detection of the embedded watermark [9]. A watermarking technique that is not robust is called fragile watermarking. Capability to recover data without original data: The amount of watermark embedded in the original host data greatly depends on the availability of the original data during the extraction of the watermark. It also affects the difficulties of the data extraction. The capability of recovering data without original data is required for applications in copyright protection, and copy tracking [10].

3. Bit rate of watermarking algorithm: The ability of embedding a significant fraction of the amount of data in the original data depends critically on the capability of the watermarking algorithm in adapting its insertion strategy to the underlying original data. In some applications, such as embedding a smaller image in a larger image or embedding multiple speech signals in a video, a large fraction of amount of data are embedded in the original data.

4. Security: In order to protect information from unauthorized user, the presence of the watermark is only detectable with a secret key. The secret key controls the insertion of the watermark in the original data. In this situation, knowing the exact watermarking algorithm does not help in extracting the watermark unless the authorized person offers the secret key. Security is necessary for applications that require protection of the watermark. Inconvert communication scenarios, the watermarking procedures may be interrupted in the same way as encryption techniques.

5. Unambiguous proof of ownership: The proof of ownership is the application that draws most attention in watermarking technologies. Unfortunately, no current watermarking technique is able to unambiguously determine the ownership of a data if it does not use the original or copy in the detection process. Watermark can be added to the watermarked data that correlates well. In such case, multiple ownership may be claimed, which is also known as a deadlock problem. Unambiguous proof of ownership is critical for copyright protection.

IV. BASIC SPREAD SPECTRUM APPROACH

The work on robust watermarking is based on spread spectrum (SS) principles. In SS watermarking, the embedded signal is generally a low energy pseudo-randomly generated white noise sequence [11]. It is detected by correlating the known watermark sequence with either the extracted watermark or the watermarked signal itself (if the host is not available for extraction). If the correlation is above a given threshold then the watermark is detected. The anti-jamming properties of SS signaling makes it attractive for application in watermarking since a low energy, and hence imperceptible, watermark, robust to narrow band interference, can be embedded. In most SS techniques [3] the pseudo-random white noise watermark sequence is added to the host signal and is detected by correlating the known watermark with the watermarked signal. That is, the watermark is embedded in some domain of the signal using linear addition. The shortcoming of such method is in the channel capacity estimate, where they used the capacity formula for a Gaussian channel, which is not the best model of the noise in a single image.

V. IMPROVED WATERMARKING TECHNIQUE BASED ON THE MDCT

Most of the watermarking techniques used for image and video format such as JPEG, MPEG-1, MPEG-2, MPEG-3, and MPEG-4 include block transformation [5, 6, 7, 8] which are lossy. This introduces unwanted artifacts such as blocking, blurring or ringing which make the reconstructed image appear different from the original image. MDCT is a lapped orthogonal transform that is widely used in signal processing [2]. These transforms perform time domain aliasing cancellation which is a good tool to analyze and synthesize signals. The proposed approach uses MDCT for transformation of images. The 50% overlap between successive blocks results in reducing the undesirable artifacts and produce very high quality images [12].

A. Modified DCT

If MDCT is performed on a sequence of data, the number of samples before and after the transformation is the same. No
single block of data after the inverse MDCT is performed resembles the original data on which the transform is applied. When these blocks of data are added after performing inverse transformation, the errors introduced by the transform cancels out due to time domain aliasing cancellation The MDCT for a two dimensional array is defined as:

\[
X(k,l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} s(i, j) \cos[\frac{\pi}{n}(2k + 1)(i + n)] 
\]

\[
\cos[\frac{\pi}{n}(2l + 1)(j + n)]
\]

Where, \(n=1/2 \lfloor n/2+1 \rfloor\)

MDCT has similar advantages over DCT. It can be implemented very effectively with FFT algorithms and its coefficients are symmetrical.

\[
x(k, l) = x(N - k - 1, N-1-l)
\]

\[
= -x(k, N-l-1)
\]

\[
= x(N-k-1,1)
\]

This reduces the spectrum size from \(N^2\) to \((n/2)^2\). The inverse MDCT is defined as

\[
Y(k,l) = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{1}{N} s(i, j) \cos[\frac{\pi}{n}(2k + 1)(i + n)]
\]

\[
\cos[\frac{\pi}{n}(2l + 1)(j + n)]
\]

VI. CONCLUSION

This study has introduced a number of techniques for the watermarking of digital images, as well as touching on the limitations and possibilities of each. Although only the very surface of the field was scratched, it was still enough to draw several conclusions about digital watermarking. The limitation of the previous scheme is its dependence on the original image for detection of the watermark, which makes it susceptible to multiple claims of ownership. From the comparisons it is shown that the correlation value of improved scheme is compared to a threshold to determine whether the received image contains the more robust watermark or not. Results were slightly higher than other schemes. Typically these techniques are computationally pricey, and unpredictable. This remains one of the major problems in the development of robust digital watermarking for digital images.

REFERENCES


