DIGITAL WATERMARKING OF MULTIMEDIA DATA

ABSTRACT

OF THE

THESIS

SUBMITTED FOR THE AWARD OF THE DEGREE OF

Doctor of Philosophy

IN

ELECTRONICS ENGINEERING

BY

FAROOQ HUSAIN

Under the Supervision of

Dr. Omar Farooq

Prof. Ekram Khan

DEPARTMENT OF ELECTRONICS ENGINEERING
Z.H. COLLEGE OF ENGINEERING AND TECHNOLOGY
ALIGARH MUSLIM UNIVERSITY
ALIGARH (INDIA)

2013
ABSTRACT

In the modern era of information technology, the use of multimedia to exchange information is increasing day by day. The digital contents are transmitted over wired/wireless networks and/or stored on storage media, for the purpose of distribution and sharing of the information. However, these contents can be easily replicated, modified and re-distributed by unauthorized third party. The ease with which digital data can be copied and manipulated has generated a need for security and authenticity of multimedia contents. Various techniques such as cryptography, steganography and digital watermarking have been used in multimedia applications to enhance the security. Cryptography deals with securing the multimedia contents by encrypting them in a noise-like pattern using a secret key. Cryptography does not completely solve the security problems because once the data decrypted, there is no control on its dissemination. Steganography is the science of hiding the existence of the message (information content) in another signal (referred to as a container or dummy signal). The container signal is just a carrier of important information content. Steganographic methods are not in general robust i.e., the hidden information can not be recovered after data manipulation. Digital watermarking has been proposed as a viable solution to improve multimedia security and to verify the authenticity of the contents while offering the robustness against any attacks. In watermarking, the additional information (watermark) is embedded into the digital contents imperceptibly such that watermark may be detected/extracted later to make an assertion about the multimedia data.

Watermarking has been proposed for various applications such as copyright protection, copy control, broadcast monitoring, content authentication, etc. A watermarking scheme should have good imperceptibility; better robustness and higher embedding capacity. A watermark is said to be imperceptible if the original host signal and its watermarked version are perceptually indistinguishable to each other. The property of resistance against distortion due to various signal processing operations applied on watermarked multimedia signal is known as robustness and the number of watermark bits embedded in a host signal without affecting its imperceptibility is called the embedding capacity or payload.
Various algorithms for digital watermarking of multimedia data such as audio, images and video have been proposed that involve embedding of watermark in the spatial, transform and compressed domains. The properties of Human Auditory System (HAS) and Human Visual System (HVS) have been explored in maximizing embedding strength without causing significant perceptual distortion.

In this thesis, digital watermarking of multimedia data, mainly for audio and images are considered. Two chapters are devoted to the audio watermarking in which two schemes namely chirp-based and wavelet function-based watermarking schemes are proposed, implemented and analyzed. Next two chapters of work deal with digital image watermarking schemes. In these schemes, imperceptibility and robustness of DFRFT domain and hybrid (DWT and DFRFT combined) domain of images are investigated. All the watermarking schemes presented in this thesis have been simulated using MATLAB software.

This thesis presents Chirp-Based Digital Audio Watermarking (CB-DAWM) scheme which uses chirp signal as watermark. Three types of chirp signals (linear, quadratic and logarithmic) have been studied. In CB-DAWM scheme, low human ear sensitivity for frequencies below 100 Hz is taken as an advantage to embed imperceptible chirp-based watermarks. This watermarking scheme has been simulated for single-level and multi-level watermark embedding to obtain multi-level security. The performance of this scheme in terms of Bit Error Rate (BER), Objective Difference Grade (ODG) using Perceptual Evaluation of Audio Quality (PEAQ) basic model, and Signal-to-Watermark Ratio (SWR) is evaluated under various audio watermarking attacks for single-level and multi-level watermark embedding schemes. The presented scheme is found to be robust against most of the audio watermarking attacks such as low-pass filtering, up-sampling by interpolation, down-sampling by decimation, re-sampling, amplitude scaling, and MP3 compression. At the same time, it shows limited robustness against high-pass filtering, band-pass filtering and AWGN attacks for both single-level and multi-level watermarking schemes. However, these schemes are not robust against cropping attack. Since multi-level CB-DAWM has different levels of robustness, therefore, it can be used to embed information having different levels of security into a host audio signal. By using multi-level CB-DAWM, the payload is increased by 39.68 % compared to single-level CB-DAWM while
maintaining imperceptibility of audio signal. Average ODG, a measure of inaudibility of watermark after one level, two levels and three levels of watermarking are -0.38, -0.46 and -0.48, respectively. These values show that imperceptibility is maintained for single-level as well as for multi-level CB-DAWM schemes.

Another audio watermarking scheme proposed in this thesis is based on wavelet function i.e., Wavelet-Based Digital Audio Watermarking (WB-DAWM) scheme. This scheme is simulated, evaluated and compared with CB-DAWM scheme. In this scheme, a Daubechies wavelet function has been used to encode watermark sequences. This scheme is found to be useful for both single-level and multi-level watermark embedding. The performances of these schemes (single-level and multi-level) are also measured in terms of average values of ODG using PEAQ basic model, SWR and BER under various audio watermarking attacks. The average ODG values for watermarked audio signals obtained using multi-level WB-DAWM after one level, two levels and three levels are -0.067, -0.078 and -0.080, respectively. These values of ODG indicate that single-level and multi-level WB-DAWM schemes are imperceptible because values of ODG are close to zero. The proposed single-level and multi-level WB-DAWM schemes are found to be resilient against various attacks such as low-pass filtering, up-sampling, down-sampling, re-sampling, amplitude scaling and MP3 compression. The WB-DAWM schemes show limited robustness against high-pass filtering, band-pass filtering and AWGN attacks. These schemes are also not robust against cropping attack. Some of the advantages of WB-DAWM schemes over CB-DAWM schemes are as follows:

Firstly, the WB-DAWM scheme (single-level and multi-level) is more imperceptible compared to corresponding CB-DAWM scheme as it gives relatively lower average value of ODG. Secondly, the wavelet-based audio watermarking scheme is more robust against high-pass filtering, band-pass filtering and AWGN attacks compared to corresponding CB-DAWM schemes. Further, single-level WB-DAWM scheme offers 19.03% increased payload with improved imperceptibility compared to single-level CB-DAWM scheme.

For a DFRFT-based image watermarking scheme, a non-blind watermark extraction scheme has been proposed. It has been assumed that the watermark is embedded by either increasing (if watermark data is '1') the values of the pre-selected
set of contiguous DFRFT coefficients or leaving them unchanged (corresponding to '0' watermark data) of host images. The proposed algorithm is then used to extract the watermark data by identifying the amount of changes in the same set of DFRFT coefficients of watermarked image compared to the corresponding DFRFT coefficients of host image. The performance of the proposed scheme has been compared with a popular DWT-based Kundur's watermarking method. Performances of both image watermarking techniques are measured in terms of Peak Signal-to-Noise Ratio (PSNR) of watermarked images. It has been observed that for a set of five test images, the average PSNR of watermarked image (for the same watermark data) is about 51.24 dB where as that for DWT-based method is about 45.14 dB. Therefore, the DFRFT based method is found to have better imperceptibility compared to DWT-based Kundur's method. The performance of proposed extraction method is also compared under various attacks and it has been observed that for attacks such as salt & peppers noise, median filtering, Additive White Gaussian Noise (AWGN) and JPEG compression, the proposed method has better robustness (measured in terms of bit error rate of extracted data). However, for some attacks such as histogram equalization and sharpening, the watermark extraction performance of DFRFT-based method is found to be inferior in comparison to DWT-based Kundur's method.

In order to improve watermark extraction performance under histogram equalization and sharpening attacks, another image watermarking scheme has been developed using a combination of DWT and DFRFT. The robustness of the algorithm for histogram equalization and sharpening attacks can be enhanced by exploiting the multi-resolution sub-band decomposition property of DWT and applying DFRFT on a high frequency sub-band or a combination of high frequency sub-bands of wavelet transformed host image. This scheme uses only one or two levels of DWT decomposition for watermark embedding. Non-blind watermark extraction scheme similar to the one described in previous paragraph is used to extract embedded watermark. Average PSNR of watermarked image obtained using proposed hybrid (combination of DWT and DFRFT) scheme is 51.35 dB, which shows imperceptible watermarking of images. Simulation results show that for histogram equalization attack, the BERs of extracted watermark for DWT and DFRFT-based methods are obtained as 44.62-48.88% and 81.55-88.87%, respectively for the considered set of images, whereas for combined DWT and DFRFT domain method, the BER is 0-
28.32%. Similarly, for sharpening attack, the BERs for DWT, DFRFT and combined (DWT and DFRFT) methods are 32.56-47.57%, 70.32-77.93% and 0-7.72% respectively. Therefore, the proposed hybrid domain watermarking method has better robustness in comparison to the watermark embedding in individual domain such as DFRFT and DWT for histogram equalization and sharpening attacks.
LIST OF PUBLICATIONS

Journal Papers (International)


Conference Papers (International and National)


Papers Communicated