Tampered Digital Image Recovery

Akhila Aniyan
PG Student
Mount Zion College of Engineering, Kadammanitta Kerala, India

Abstract

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as an audio, video or image data. It is typically used to identify ownership of the copyright of such signal. Watermarking is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to, contain a relation to the 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. It is prominently used for tracing copyright infringements and for bank note authentication. We apply the wavelet transform and set partitioning in hierarchical transforms (SPIHT) source encoding method to efficiently compress the original image. Tampered area can be detected by using watermarking algorithm.

Keywords: SPIHT, Digital watermarking, DCT, DWT, Spatial domain, Least Significant Bit (LSB)

I. INTRODUCTION

Digital image processing is a rapidly developing area with various raising applications in computer science and engineering. It is very important field for the research work because its techniques are used in almost all kinds of tasks like human computer interface, medical visualization; image enhancement, Law enforcement, artistic effects, image restoration and digital watermarking for security purpose. One common approach is to use the hash of the original image. The receiver declares the image as unaltered if the hash output is the same as the one transmitted from the original image. The digital watermarking is a process of information hiding. There are various techniques for hiding the information in the form of digital contents like image, text, audio and video. Basically digital watermarking is a method for embedding some secret information and additional information in the cover image which can later be extracted or detected for various purposes like authentication[5], owner identification, content protection and copyright protection. Digital Watermarking works by concealing information within digital data, such that it cannot be detected without special software with the purpose of making sure the concealed data is present in all copies of the data that are made whether legally or otherwise, regardless of attempts to damage/ remove it. Another class of watermarking techniques takes one step further and aims to accomplish both tasks of tampering localization and error concealment via a single watermark

II. WATERMARK EMBEDDING AND RECOVERY USING DCT-DWT

Watermarking algorithm[1] by using transform domain techniques embedding information into the frequency domain. The most popular transforms where the frequency domain watermarking algorithms work are Discrete Fourier Transform (FT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). DFT decompose image in sine and cosine form. DFT gives output in complex value and it required more frequency rate. DFT is not used now days due to above disadvantages. Discrete Cosine Transformation (DCT) transforms a signal from the spatial into the frequency domain by using the cosine waveform. DCT divide the information energy in the bands with low frequency and DCT popularity in data compression techniques such as JPEG and MPEG. The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of the image. Here the middle frequency bands chosen such that they minimize to avoid the visual important parts of the image. The basic idea of the DWT we focus on one dimensional signal. A signal splits into two parts, usually high frequencies and low frequencies. This process is continuing until the signal has been entirely decomposed or stopped before by the application at hand. For compression and watermarking applications, generally no more than four decomposition steps are computing. Furthermore, from the DWT coefficients, the original signal can be reconstructing. The reconstruction process called the inverse DWT (IDWT).
Fig. 1: Watermark Embedding using DCT-DWT

Fig. 2: Watermark Recovery

In watermark recovery procedure, the host image is decompose through DWT transform and select the appreciate wavelet modulus in the frequency level. The watermarked image will be Discrete Cosine Transformed. Because the DCT modulus contain the low frequency information of watermarking image, as long as these information do not lose or lose little then the watermarking image can be renewed well. This enhances the robustness and concealment.

III. PROPOSED SYSTEM

The goal of watermarking is to embed a watermark into original image to protect it against tampering. It means that the watermark must be capable of both finding the tampered areas of the received image, and recovering the content of the original image in those zones. In order to achieve this goal, we keep mm most significant bits of each pixel unchanged, and use the remaining nw bits for the watermark embedding.

For the purpose of image recovery, compress the image using a source encoding algorithm, and embed the result as watermark. However, some of compressed image information might be lost because of image tampering[2]; hence the compressed image bit stream must be channel coded to exhibit robustness against a certain level of tampering. In order to detect tampered blocks at the receiver, some check bits are generated from those parts of image which remain unchanged during watermark embedding procedure. These check bits are inserted as a part of total watermark. As a result, the least significant bits (LSB) are comprised of both channel coded bits and check bits.
Having tampered blocks known using the check bits, tampering can be modeled as an erasure error. Therefore, compressed bit stream is channel coded using a code capable of resistance against certain level of erasure. At the receiver, the check bits locate tampered blocks.

![Fig. 3: Proposed watermark embedding using two LSB.](image)

Fig. 3: Proposed watermark embedding using two LSB.

![Fig. 4: Tampering detection and image recovery scheme using 2 LSB.](image)

Fig. 4: Tampering detection and image recovery scheme using 2 LSB.

The original image is source coded using SPIHT compression algorithm. The source encoder output bit stream is channel coded using RS code of a required rate and over appropriate field. The lengths of the channel encoder input and output blocks are also taken as long as possible to accomplish the best performance. Setting up the RS channel codes over GF(2t +1) instead of G(2t ) is another suggestion of this paper which greatly simplifies the complexity of channel encoder and decoder implementation. SPIHT is an embedded compression algorithm, that is, one can truncate its output bit stream at the desired rate and come to a certain reconstruction of the original image. The more output rate exploited, the better quality of reconstruction is achievable. To satisfy this goal, the algorithm[3] sorts the rounded multi-resolution wavelet transform coefficients according to their magnitudes and transmits them based on significant bit order. The sorting order must be available to the decoder as well. The maximum achievable peak signal to noise ratio (PSNR) of our reconstruction algorithm happens when channel code has worked absolutely and retrieved all source encoded bits, and equals the PSNR of SPIHT for original image at the rate of ns . For instance, SPIHT offers the PSNR of 44.9 dB for the Cameraman image when compressed at the rate of 1 bpp.
As a consequence, if we set \( ns = 1 \) in our algorithm, no PSNR recovery of more than 44.9 dB is achievable. RS codes are directly feasible for every \((n, k)\) where \( n \) divides \( 2t - 1 \) (maximum order of the field members). Otherwise, encoder and decoders are implemented by puncturing a mother \( RS(m, k) \) code where:

\[
m = \min m'(m'\mid 2t - 1 \text{ and } m' > n).
\]

The row-column indices of these blocks are used to generate brc position bits. bh generated hash bits are XORed with a binary random bh-bit key which is constant over the whole image. bh resulted check bits are inserted in the corresponding block along with bc channel code bits as the image watermark. At the receiver, the check bits are extracted and XORed with the hash bits generated in a way similar to the embedder.

### IV. Simulation Result

Generally, the accurate measurement of the imperceptibility as perceived by a human observer is a great challenge in image/video processing. The reason is that the amount and visibility of distortions introduced by the watermarking attacks strongly depend on the actual image/video content [23]. To measure the perceptual quality, we calculate the peak to signal-to-noise ratio (PSNR) that is used to estimate the quality of the watermarked frames in comparison with the original ones. The PSNR [24] is defined as follow:

\[
PSNR = 20 \log(\text{max}/\sqrt{\text{MSE}})
\]

The extraction process shows that the size of obtained watermark is changed, because the watermark image is extracted from the low-frequency part of original frames, so the size of the extracted information is 1/4 of the original frames size, that is, the extracted watermark stays at the position where it is embedded in the original frames. Fig. 6 shows this matter. So this algorithm can help us observe the specific location of the watermark embedded frames. In short, this algorithm provide a new approach for digital video watermarking research and practice, therefore it is of great practical significance.

![Fig. 5: Enter the input image: ‘football.jpg’](image1)

![Fig. 6: Enter the watermark image: ‘best.bmp’](image2)
Fig. 7: Comparison of two methods

Fig. 8: The bar graph of existing method

Fig. 9: The bar graph of proposed method
V. APPLICATIONS

Digital watermarking provides an added layer of security to the content protection chain to deter unauthorized use of content by embedding watermarks that identify the permitted uses of the content into the music or motion picture soundtrack prior to theatrical, packaged media (Discs, DVDs) and online digital distribution. Devices read the watermark during playback or copying of content. If the watermark indicates that the use is unauthorized, the playback or copying is stopped or the audio is muted, and an explanatory message may be displayed. Forensic watermark applications enhance a content owner’s ability to detect and respond to misuse of its assets. Forensic[4] watermarking is used not only to gather evidence for criminal proceedings, but also to enforce contractual usage agreements between a content owner and the people or companies with which it shares its content. It provides positive, irrefutable evidence of misuse for leaked content assets. Digital watermarks offer new opportunity for content owners, advertisers and more generally marketers looking for new ways to engage consumers with richer media experiences from the STB and Television set.

VI. FUTURE SCOPE

Nowadays, there is a constant competition between a watermark embedder and an adversary. Due to the rapid expansion of new, dynamic, and complex watermarking applications, fixed watermarking strategies may become obsolete. Few potential watermarking applications, where dynamic and adaptive watermarking strategies are highly desirable are: print-to-web technology, transaction tracking, broadcast monitoring, securing data sent through context aware medical networks, secure digital camera, data transmission through wireless networks, agent based online auction systems etc. Such watermarking applications have to be guarded against both intentional and unintentional attacks that may change with respect to time. In cases, where the type of attack is the same, but only its intensity changes with time, the retraining of only the machine learning based decoding model is recommended. There may be no need of the retraining of the GP based embedding phase. However, in applications, where the type of attack also changes dynamically, then both embedding and decoding models should be retrained for coping with the distortions introduced by the dynamic attacks. The only drawback of the proposed system is that it is not suitable for geometric attacks, which constitute an important class of attacks. In future, we aim to develop appropriate VTFs that counter geometric attacks as well. For this purpose, statistical moments can be utilized.

REFERENCES