Digital Watermarking

Mrs Megha Kolhekar.*, Mrs. Anita Jadhav**
**Assistant Professor, **Lecturer,*
Electronics and Telecom Department,
Fr. C. Rodrigues Institute Of Technology
Vashi, Navi Mumbai

Abstract

The growth of networked multimedia systems has created the need for the copyright protection of various digital medium, e.g. images, audio clips, video, etc. Copyright protection involves the authentication of ownership and the identification of illegal copies of a (possibly forged) image. One approach used to address this problem is to add a visible or invisible structure to an image or video that can be used to seal or mark it. These structures are known as digital watermarks. The watermark is capable of carrying such information as authentication or authorization codes, or a legend essential for image interpretation.

In this paper, we briefly describe watermarking system and discuss a method to embed visible and invisible watermark in video.

1. INTRODUCTION

1.1The need for watermarking

A great deal of information is now being created, stored, and distributed in digital form. Newspapers, and magazines, for example, have gone online to provide real-time coverage of stories with high-quality audio, still images, and even video sequences. The growth in use of public networks such as the Internet has further fueled the online presence of publishers by providing a quick and inexpensive way to distribute their work. The explosive growth of digital media is not limited to news organizations, however. Commercial music may be purchased and downloaded of the Internet, stock photography vendors digitize and sell photographs in electronic form, and Digital Versatile Disc (DVD) systems provide movies with clear images and CD-quality sound.

Digital watermarking is seen as a partial solution to the problem of securing copyright ownership. Essentially, watermarking is defined as the process of embedding sideband data directly into the samples of a digital audio, image, or video signal. Sideband data is typically "extra" information that must be transmitted along with a digital signal, such as block headers or time

watermark is not transmitted in addition to a digital signal, but rather as an integral part of the signal samples. The value of watermarking comes from the fact that regular sideband data may be lost or modified when the digital signal is converted between formats, but the samples of the digital signal are (typically) unchanged[3].

Watermarking techniques can complement encryption by embedding a secret imperceptible signal, a watermark, directly into the clear data in such a way that it always remains present. Such a watermark can for instance be used for the following purposes [3]:

1.1.1 Copyright protection: The underlying strategy consists in embedding a watermark, identifying the copyright owner, in digital multimedia data. The rightful owner can show the watermark in case of a dispute. Watermarking algorithms are consequently required to be non-invertible in order to provide copyright protection services especially in cases of multiple ownership issues.

1.1.2 Fingerprinting [5]: Electronic distribution of content allows each copy distributed to be customized for each recipient. This allows a unique watermark to be embedded in the copy of each customer like customer name or ID. This allows the distribution companies to track down the source of illegal copy in case of a leakage. Another important issue is the illegal copying of brand new movies projected onto cinema screens by means of a handhold video camera. A watermark can be embedded during the show time identifying the cinema, the presentation date and time. If the illegal copy created with a video camera is found, the watermark is extracted and the cinema to blame is identified.

1.2. Watermarking requirements [1]

Each watermarking application has its own specific requirements. Therefore, there is no set of requirements to be met by all watermarking techniques. Nevertheless, some general directions can be given for most of the applications mentioned above:

1.2.1. Perceptual transparency: In most applications the watermarking algorithm must embed the watermark such that this does not affect the quality of the underlying host data. A watermark-embedding procedure is truly imperceptible if humans cannot distinguish the original data from the data with the inserted watermark.

1.2.2. Payload of the watermark: The amount of information that can be stored in a watermark depends on the application. For copy protection purposes, a payload of one bit is usually sufficient.

1.2.3. Robustness: It accounts for the capability of hidden data to survive host signal manipulation, including both non-malicious manipulations, which do not explicitly aim at removing the watermark or at making it unreadable and malicious manipulations, which precisely aims at damaging the hidden information. We can consider four qualitative levels encompassing most of the situations encountered in practice.

1.2.4. Secure watermarking: The loss of the hidden data should be obtainable only at the expense of significant degradation of the quality of the host signal.

1.2.5. Semi-fragile watermarking: Some applications does not require robustness as major requirement .We say that watermark is semi-fragile if it survives only a limited, well specified, set of manipulations leaving the quality of the host document virtually intact.

1.2.6. Fragile watermarking: A watermark is said to be fragile, if the information hidden within the host data is lost or irremediably altered i.e. only part of the watermark is damaged. A fragile watermark that has to prove the authenticity of the host data does not have to be robust against processing techniques or intentional alterations of the host data, since failure to detect the watermark proves that the host data has been modified and is no longer authentic. [3].

1.2.7. Security: The security of watermarking techniques can be interpreted in the same way as the security of encryption techniques. According to Kerckhoff's Principle, one should assume that the method used to encrypt the data is known to an unauthorized party, and that the security must lie in the choice of a key. Hence a watermarking technique is truly secure if knowing the exact algorithms for embedding and extracting watermark does not help an unauthorized party to detect the presence of the watermark.

2. Existing Methods

Many digital watermarking schemes have been proposed in the literature for still images and videos. Most of them operate on uncompressed videos, while others embed watermarks directly into compressed video. Recently, there are investigations in video watermarking techniques that are robust and invisible. These schemes can be distinguished in terms of the domain that the watermark being embedded or detected, their capacity, real-time performance, the degree to which all three axes are incorporated, and their resistance to particular types of attacks. A classification map of the existing video watermarking techniques is presented in Figure 2. They can be divided into 3 main groups based on the domain in which the watermark is embedded; they are the spatial domain, the frequency domain and the MPEG coding structure based method [3].

2.1 Spatial Domain Watermarks

We first review the video watermarking techniques in the spatial domain. Algorithms in this class generally share the following characteristics:

- The watermark is applied to the pixel or coordinate domain.
- No transforms are applied to the host signal during watermark embedding.

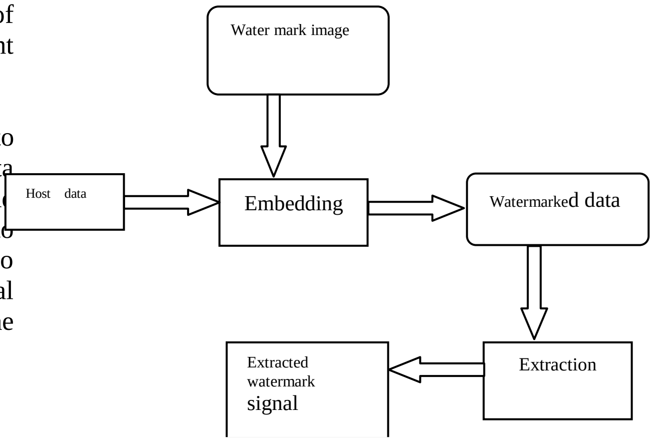


Figure 3. Basic watermarking process

The watermark is derived from the message data via spread spectrum modulation.

- Combination with the host signal is based on simple operations, in the pixel domain.
- The watermark can be detected by correlating the expected pattern with the received signal.

Several different methods enable watermarking in the spatial domain [3], as described below:

2.1.1.Correlation-Based Techniques

Another technique for watermark embedding is to exploit the correlation properties of additive pseudo-random noise patterns as applied to an image. A pseudo-random noise (PN) pattern W(x,y) is added to the cover image I(x,y), according to the equation shown below in Equation (1):

$$Iw(x,y)=I(x,y)+kW(x,y) \qquad (1)$$

In Equation (1), k denotes a gain factor, and Iw the resulting watermarked image. Increasing k increases the robustness of the watermark at the expense of the quality of the watermarked image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and the watermarked image is computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set. This method can easily be extended to a multiple-bit watermark, this is done by dividing the image into blocks, and performing the above procedure independently on each block. This basic algorithm can be improved in a number of ways. First, the notion of a threshold being used for determining a logical '1' or '0' can be eliminated by using two separate pseudorandom noise patterns. One pattern is designated as a logical '1' and the other a '0'. The above procedure is then performed once for each pattern, and the pattern with the higher resulting correlation is used. This increases the probability of a correct detection, even if the image has been subjected to an attack .

2.1.2. Least Significant Bit Modification

The simplest example of a spatial domain watermarking technique that is not based on correlation is the LSB (least significant modification) method. If each pixel in a grey level image is represented by an 8-bit value, the image can be sliced up in 8 bit planes.

Since the least significant bit plane does not contain visually significant information it can easily be replaced by an enormous amount of watermark bits. More sophisticated watermarking algorithm that makes use of LSB modification are found in [8]. In fact these watermarking techniques are not very robust to processing technique because the LSB plane can be easily replaced by random bits, effectively removing the watermark.

2.2.Frequency Domain Watermarks

Generally DCT, FFT and wavelet transform are used as the methods of data transformation.

The main strength offered by transform domain techniques is that they can take advantage of special properties of alternate domains to address the limitations of pixel-based methods or to support additional features. For instance, designing a watermarking scheme in the DCT domain leads to better implementation compatibility with popular video coding algorithms such as MPEG. The frequency domain watermarking schemes are relatively more robust than the spatial domain watermarking schemes, particularly in lossy compression, noise addition, pixel removal, rescaling, rotation and shearing. Generally, the main drawback of transform domain methods is their higher computational requirement. We discuss the details of three methods here: Discrete Cosine Transform, Discrete Wavelet Transform, and Discrete Fourier Transform.

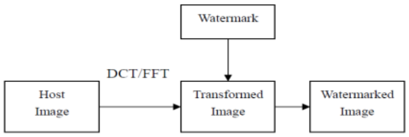


Figure 4.Watermarking in frequency domain[5]

2.2.1 Discrete Cosine Transform

The classic and still most popular domain for image processing is that of the Discrete Cosine Transform, or

DCT. 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 an image. The middle frequency bands are chosen such that they have minimize they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies) .

In DCT domain we can have a 2-D watermark signal W, which is embedded in the middle band frequency of 8 × 8 DCT block. The 8 × 8 DCT coefficients F(u,v) are modulated according to the following equation:

$$IWx,y = (Ix,y(u, v) + k \_Wx,y(u, v) \qquad \text{if } u, v\ \varepsilon\ FM$$
$$=Ix,y(u, v) \qquad \text{if else} \qquad (2)$$

Here FM denotes the middle band frequency coefficients, k the gain factor, (x,y) thespatial domain location of an 8×8 pixel block in image I and (u,v) the DCT coefficientsin the corresponding 8 × 8 DCT block.

2.2.2.Discrete Wavelet Transform

Another possible domain for watermark embedding is that of the wavelet domain. The DWT (Discrete Wavelet Transform) separates an image into a lower resolution approximation image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The process can then be repeated to compute multiple scale wavelet decomposition, as in the shown below in Figure 5.

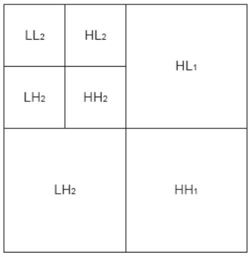


Figure5. Multiple scale

One of the most straightforward techniques is to use an embedding technique similar to that used in the DCT. This can be easily extended to multiple bit messages by embedding multiple watermarks into the image. As in the spatial version, a separate seed is used for each PN sequence, which are then added to the detail coefficients.

During detection, if the correlation exceeds the threshold for a particular sequence, a '1' is recovered; otherwise a zero. The recovery process then iterates through the entire PN sequence until all the bits of the watermark have been recovered.

2.3 Spread spectrum techniques

In spread spectrum communications, one transmits a narrowband signal over a much larger bandwidth such that the signal energy present in any single frequency is undetectable. Similarly, the watermark is spread over many frequency bins so that the energy in any one bin is very small and certainly undetectable.

The mostly described spread spectrum techniques are Direct Sequence Spread Spectrum (DS-SS) and Frequency Hopping Spread Spectrum (FH-SS) techniques. In the DS-SS algorithm, a low level wideband signal can be easily hidden within the same spectrum as a high power signal, which each signal appears to be noise to the other. The core component of these spread spectrum systems is a Pseudo Random Noise Sequence (PRNS). For these direct sequence spread spectrum systems, the original baseband bit stream is multiplied by the PRNS to produce a new bit stream. Only those receivers equipped with correct PRNS can decode the original image.

The FH-SS algorithm involves a periodic change of transmission frequency. The set of possible carrier frequencies is called the hopset. Hopping occurs over a frequency band that includes a number of channels. Each channel is defined as a spectral region with a central frequency in the hopset.Data is therefore sent by hopping the transmitter carrier to seemingly random channels which are known only to the desired receiver. On each channel, small bursts of data are sent using conventional narrowband modulation before the transmitter hops again.

The DS-SS technique is used in the process of watermarking generating to provide robustness to the embedded signal, while the FH-SS technique is utilized to determine the embedding positions in an original image [2].

Firstly, a sequence of information bits, consisting of '-1' and '1', is spread by multiplying with a large factor, called the chip-rate C_r, to obtain the spread information sequence. The size of this sequence is equal to the value of chip-rate multiplied by number of information bits. The spread sequence is then modulated with a binary pseudo-noise sequence to yield the modulated spread sequence, and is finally amplified with a locally adjustable amplitude factor to obtain the watermark signal. The block diagram of watermark process is illustrated in the block A of Fig. 6.

Each bit of the watermark signal will be embedded into some assigned locations, which is randomly determined by a key-based FH-SS technique, within the image frame, instead of whole frame. Therefore, each watermark bit will only be dispersed over its corresponding locations within some parts of the image. The block diagram of location determining process is shown in the block B of Fig.6. [2].

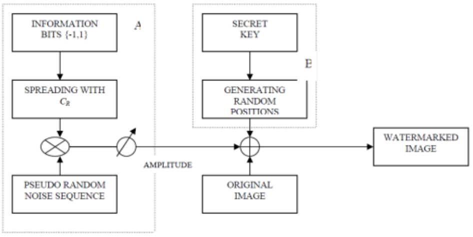


Figure 6.Spread spectrum embedding [2]

3. IMPLEMENTATION

One of the goals of this seminar is to implement two forms of watermarking techniques, one invisible and the other visible. We have used 'MATLAB' software for this implementation.

3.1 Invisible Watermarking (Bit plane watermarking)

Host data: video

Watermark data: image

1. A raw video 'A' is selected from the set of videos. Let this be the base video in which the watermark is embedded. Size: [mXnX3Xf], f: number of frames, 3: RGB, mXn: size of each frame.

2. A raw bitmap/ png/ jpeg image 'B' is be selected from the set of images. This is the watermark image. Size: iXj

3. Calculate the number of frames of the video required to accommodate the watermark as:

Let 'V' represent intensities of video frame pixels.

V(1,1), V(1,2),……………….V(1,m)
V(2,1), V(2,2),……………….V(2,m)
.
.
V(f,1), V(f,2)………………….V(f,n)

Let 'I' represents intensities of image.

I(1,1)……………………………I(I,j)

$I(1,1)= I_B(1……8)$ 8-bit binary pixel

Now $I_B(1)=V(1,1)_{LSB}$
$I_B(2)=V(1,2)_{LSB}$
.
$I_B(8)=V(1,8)_{LSB}$.

Thus accommodate 1 binary pixel can be put in 8 video pixels.

4. Convert the intensities of video and image into binary values. Replace the Least significant bit of 'A' with bit of image 'B'.

5. Thus 'A' is be watermarked with 'B' resulting in a combined video 'C'.

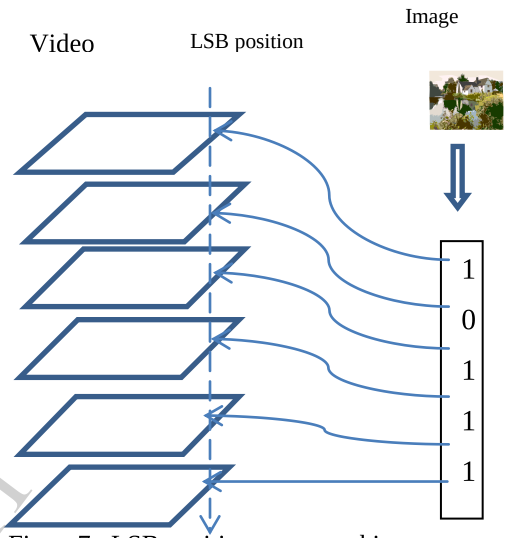


Figure7. LSB position watermarking

3.2 Visible Watermarking

Host data: video

Watermark data: image

1. A raw video 'A' is selected from the set of videos. Let this be the base video on which the watermark is embedded.
2. A raw bitmap/ png/ jpeg image 'B' is be selected from the set of images. This is be the watermark image..
3. Separate the RGB components of video and image, store it in separate matrices.
4. Select the position in video where the watermark is be placed
5. Replace the 'R' component of video with 'R' component of image at preselected position. Repeat this step for 'G' as well as for 'B' component.
6. Combine all the new RGB components of video. This is the new watermarked video.

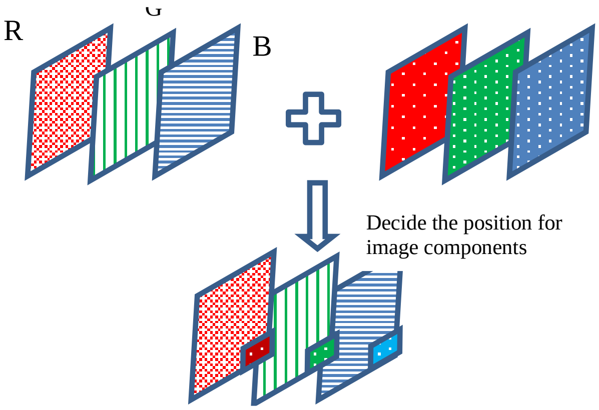


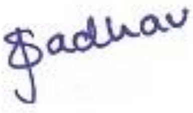
Figure8. Direct substitution watermarking

4. RESULTS

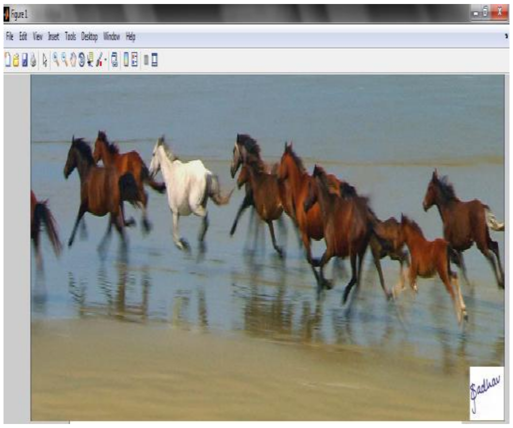
For visible watermarking:

Actual video:

Watermark image:



Watermarked video:



Mean square error:0.0139

For invisible watermarking:

Actual video

Watermark image

Watermarked video

Mean square error: 0.2439

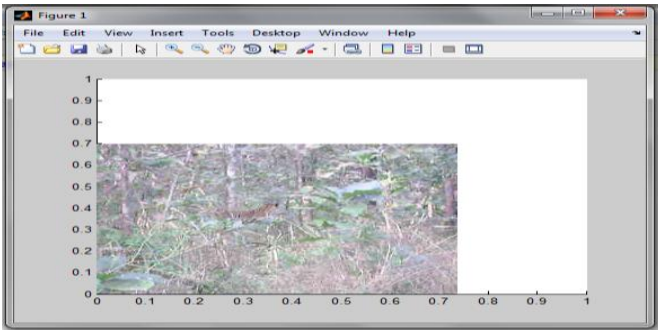


Figure 1
File Edit View Insert Tools Desktop Window Help
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1