Research Paper

IMAGE WATERMARKING FOR IMAGES CAPTURED BY DIGITAL CAMERA

[1]Poonam N. Mahamuni, [2]Prof. R.T. Patil, [3]Mr. S. P. Adure

Address for Correspondence

[1]P.G. Student, RIT, Sakharale, India and Faculty RMCET, Ambav (Devrukh)

[2]E& Tc Department, RIT, Sakharale India

[3]E& Tc Department, RMCET, Ambav (Devrukh)

ABSTRACT

The growth of computer networks has boosted the growth of the information technology sector to a greater extent. Thus the digital information which includes images, videos, text etc is readily available to anyone. At the same time care is taken to prevent the unauthorized use of the images commercially. To satisfy these need owners moved towards watermarking. In his paper the embedding technique for watermarking is presented based on LSB & DCT transforms. Here we classify the techniques based on different domains in which data is embedded. The survey is limited to images only.

KEY WORDS: Watermarking, DCT, LSB, spatial domain, frequency domain.

I. INRODUCTION

The rapid expansion of the Internet in the past years has rapidly increased the availability of digital data such as audio, images and videos to the public. Thus the problem of protecting multimedia information becomes more and more important. The digital watermarking is probably the one that has received most interest to protect data from false duplication. Watermarking is a branch of information hiding which is used to hide proprietary information in digital media like photographs, digital music, or digital video [1][2]. Digital watermarking is defined as a process of embedding data (watermark) into a multimedia object to help to protect the owner's right to that object. The embedded data (watermark) may be either visible or invisible. Images can be processed in two main approaches as spatial domain & frequency domain approach. The paper is organized in the following sections. In Section II we describe digital watermarking Techniques & section III describes watermarking process. Section IV gives the watermarking algorithm based on LSB embedding. In Section V we discuss the DCT domain watermarking. In Section VI gives some performance measure parameters for watermarking. We conclude this paper in section VII where we give the best suitable technique for digital watermarking.

II. DIGIAL WAERMARKING TECHNIQUES

The techniques proposed so far can be divided into two groups according to the embedding domain.

1 Spatial-domain approach.[2]

It is the earliest technique. Spatial domain watermarking is performed by modifying values of pixel color samples of a video frame.

1. Frequency domain approach.[2][4]

These methods are similar to spatial domain watermarking in that the values of selected frequencies can be altered. Images are converted in frequency form by using different available transforms like DFT, DCT, DWT & many others. Because high frequencies will be lost by compression or scaling, the watermark signal is applied to lower frequencies, or better yet, applied adaptively to frequencies containing important elements of the original picture. Upon inverse transformation, watermarks applied to frequency domain will be dispersed over the entire spatial image, so these methods are not as susceptible to defeat by cropping as the spatial technique.

Watermarking can be classified accordingly as

1. Private or non-blind watermarking- original cover data is required for extraction/detection of original cover data.
2. Semi-private or semi-blind watermarking- same like private. It also requires original cover data for detection of watermark.
3. Public or blind watermarking- in this neither cover data nor embedded watermark is required.

III. DIGIAL WAERMARKING PROCESS

The process of embedding a watermark in a multimedia Object is termed as watermarking. Watermark can be considered as a kind of a signature that reveals the owner of the multimedia object. Content providers want to embed watermarks in their multimedia objects (digital content) for several reasons like copyright protection, content authentication, tamper detection etc. A watermarking algorithm embeds a visible or invisible watermark in a given multimedia object. The embedding process is guided by use of a secret key which decided the locations within the multimedia object (image) where the watermark would be embedded. Once the watermark is embedded it can experience several attacks because the multimedia object can be digitally processed. The attacks can be unintentional (in case of images, low pass filtering or gamma correction or compression) or intentional (like cropping). Hence the watermark has to be very robust against all these possible attacks. Watermark embedding & detection is shown in Fig.1.

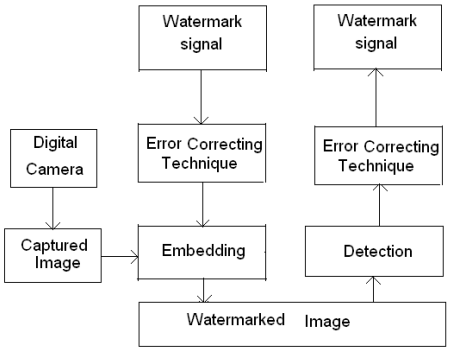

Fig.1: Watermark embedding & detection

Digital watermarking has mainly three stages.

Generation and Embedding

Random number, Pseudo Random Sequence, binary sequence and some other signals are used for watermark generation. The embedding process can be understood as the combination of watermark signal and original image.

Distribution and Possible Attacks

The distribution process can be seen as the transmission of the signal through the watermark channel. Possible attacks in the broadcast channel may be intentional or unintentional as mentioned above.

Detection

Detection process allows the owner to be identified and provides information to the intended recipient. There are two kinds detection: Informed detection and Blind detection

IV. ALGORITHM BASED ON LSB

The LSB algorithm is based on embedding of watermarked data in Least Significant Bit position of original image [4]. Here Least Significant Bit position is chosen to embed data because it contains visually insignificant information. To embed data the MSB of watermark image is stored at Least Significant Bit position of original image [6]. To retrieve data the Least Significant Bit position of original image is extracted that means the MSB of watermark image is extracted from LSB of original image. In LSB technique the data is embedded additively or linearly as follows:

$$W(x, y) = I(x, y) + k\, M(x, y)$$

Where, W(x,y) is watermarked image, I (x, y) is cover image, k is scaling factor which determines the strength of watermark in watermarked image & M(x, y) is the message image.

The steps for algorithm are

1. Load image captured by digital camera.
2. Load another image as a watermark data.
3. Replace LSB of original image by MSB of watermark data. Here we can use more than one number of bits from message image to embed in cover image as shown below:
    1. Bits used:1
        a. Host Pixel: **1011001**1
        b. Message Pixel: **0**1111100
        c. New Image Pixel: **10110010**
    2. Bits used:
        a. Host Pixel: **1011**0011
        b. Message Pixel: **0111**1100
        c. New Image Pixel: **10110111**
    3. Show original & watermark image.
    4. If the numbers of bits inserted are known then by using extraction function we get watermark data i.e. message image.

In this example an image has been hidden, the least significant bits could be used to store text or even a small amount of sound.

Limitations of LSB embedding:-

1. This method works well when both the host and secret images are given equal priority. When one has significantly more room than another, quality is sacrificed.
2. However this technique makes it very easy to find and remove the hidden data.

VI. DCT DOMAIN WAERMARKING

The discrete cosine transform (DCT) is used to transform a signal from the spatial domain into the frequency domain. The reverse process, that of transforming a signal from the frequency domain into the spatial domain, is called the inverse discrete cosine transform (IDCT) [4][6]. A signal in the frequency domain contains the same information as that in the spatial domain. The order of values obtained by applying the DCT is coincidentally from lowest to highest frequency [3][4]. The discrete cosine transform (DCT) represents an image as a sum of sinusoids of varying magnitudes and frequencies. It supports block based transform like (8x8, 16x16, 32x32 etc.). It also compacts energy of each block according to its frequency content. The two-dimensional DCT [4] is defined as follows.

$$F(u,v) = \alpha(u)\,\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

For u, v = 0, 1,2,…..,N-1 &

The inverse transform is defined as

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\,\alpha(v)F(u,v)\cos\left[\frac{(2x+1)u\pi}{2N}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

For x, y = 0, 1,2,…..,N-1

To increase robustness of watermarking the message image bits are embedded using DCT domain. Horizontal frequencies increase from left to right, and vertical frequencies increase from top to bottom. Watermark is embedded in mid & high frequency components because low frequency components are subject to heavy quantization. Hiding via a DCT is useful as someone who just looks at the pixel values of the image would be unaware about watermark. Also the hidden data can be distributed more evenly over the whole image in such a way as to make it more robust. The embedding algorithm is described below.

DCT based watermarking algorithm:

- Load image captured by digital camera.
- Load another image as a watermark.
- Divide image to be watermark i.e. cover image in 8x8 blocks.
- Apply DCT on each block.
- Embed watermark image data in frequency component.
- After this IDCT is applied to get original image which is now watermarked.

Disadvantages of DCT:

- Only spatial correlation of the pixels inside the single 2-D block is considered and the correlation from the pixels of the neighboring blocks is neglected.
- Impossible to completely de-correlate the blocks at their boundaries using DCT.
- Undesirable blocking artifacts affect the reconstructed images or video frames. (High compression ratios or very low bit rates).
- Does not perform efficiently for binary images (fax or pictures of fingerprints) characterized by large periods of constant amplitude (low spatial frequencies), followed by brief periods of sharp transitions

X. PERFORMANCE MEASURE

Peak Signal to Noise ratio used to be a measure of image quality. Signals can have a wide dynamic range, so PSNR is usually expressed in decibels, which is a logarithmic scale. PSNR is calculated by following formula [4].

PSNR in decibels (dB) is given below as:

$$PSNR = 10 \log 255^2 / MSE$$

$$MSE = 1/MN \sum \sum (x(m,n) - x^(m,n))$$

Where,

x(m,n)= original image

x^(m,n)= reconstructed image

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human observers.

XI. CONCLUSION

Digital watermarking technology has emerged as an effective means to hide copyright information in the original content to protect the authenticity of the intellectual property. In this paper we surveyed current digital watermarking techniques. Watermarking algorithms are classified according to transforms in which watermark is embedded. LSB is a spatial domain approach. 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.

REFERENCES

1. "A Survey of Digital Image Watermarking Techniques" Vidyasagar M. Potdar, Song Han, Elizabeth Chang, 3rd International Conference on Industrial Informatics, 2005 IEEE.
2. Digital Watermarking Techniques, Avani Bhatia, Mrs.Raj Kumari U.I.E.T, Panjab University.
3. Digital Image Processing- By R. Gonzales, R. Woods- Pearson Education
4. Image Processing using MATLAB codes by Dhananjay Theckedath
5. "Steganography And Digital Watermarking", Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The University of Birmingham, 2004.
6. "Watermarking algorithms using DCT & LSB replacement" by Mona M. El-Ghoneimy
7. "Performance Analysis of Digital Watermarking Techniques combined over individual DWT " by A.M.Kothari, A.C.Suthar, R.S.Gajre.
8. "Watermarking Algorithm Research & Implementation based on DCT" by G.Zhu Nong Sang. World Acedemic of science, Engineering & Technology-2008.
9. "A Dual Digital Image Watermarking Technique" by M. Sharkas, D. Elshafie & N. Hamdy. . World Acedemic of science, Engineering & Technology-2005.
10. "A DCT Domain Visible Watermarking Techniques for Images" by S.P. Mohanty, K.R. Ramakrishnan & M.S. Kankanhali.
11. "A Study on Digital Watermarking Techniques" L. Robert, & T.Shanmugapriya, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009