IOSR Journal of Electronics and Communication Engineering (IOSRJECE)
ISSN : 2278-2834 Volume 1, Issue 5 (May-June 2012), PP 11-15
www.iosrjournals.org

Analysis of Image Watermarking: LSB Modification and Spread-Spectrum Technique

Ruby Shukla, Manish, Prof. A.K. Arora
(ABES Engineering College, Ghaziabad)
EC Department, Mahamaya Technical University
Noida, U.P

Abstract: *With the growing popularity of digital Medias through the WWW, intellectual property needs copyright protection, prevention of illegal copying and verification of content integrity. The new data hiding techniques need to be developed that satisfy the requirements of imperceptibility, robustness, capacity, or data hiding rate and security of the hidden data in order to keep the distribution of digital multimedia work both profitable for the document owner and reliable for the customer. The LSB Modification and DCT are two techniques are analyzed by using various distortion metrics to verify the methods for their robustness*
Keywords*: Image watermarking, Discrete Cosine Transform, Robustness*

I. INTRODUCTION

Watermarking encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Creative methods have been devised in the hiding process to reduce the visible detection of the embedded messages.

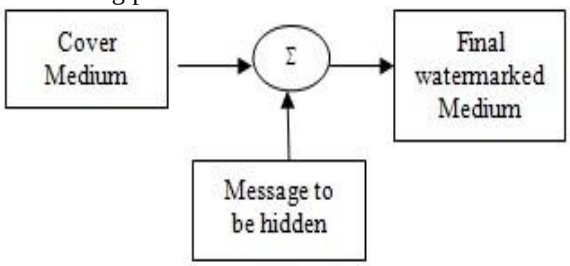


Figure1.Basic Watermarking

Watermarking is basically the process of passing information, called a *watermark*, in a manner that the very existence of the message is unknown. The aim of watermarking is to avoid drawing suspicion to the transmission of the watermark, while providing some added value to the *covering* media. The process of watermarking involves intentionally modifying the *cover* media to embed a watermark and a *secret key* to form a composite *watermarked* signal. Hiding information, where electronic media are used as such carriers, requires alterations of the media properties may introduce some form of degradation. If applied to images that degradation, at times, may be visible to the human eye and point to signatures of the watermarking methods and tools used. These signatures may actually broadcast the existence of the embedded message purpose of watermarking, which is hiding the existence of a message.

Watermarking is very similar to steganography in a number of aspects. Both seem to embed information inside a cover message with little or no degradation of the cover media. Watermarking however adds the additional requirement of robustness. An ideal steganographic system would securely add large amount of information to the cover media without causing any visual degradation. Whereas an ideal watermarking system would embed an amount of information that could not be removed or altered without making the cover object entirely unusable. A watermarking system would thus trade capacity and even security for additional robustness.

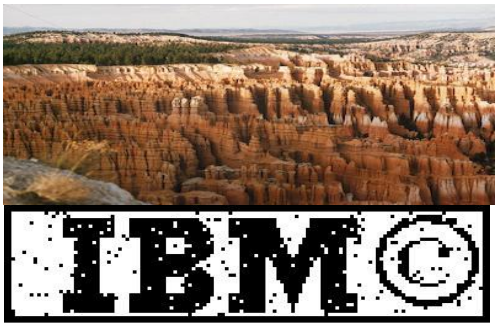
II. TYPES OF WATERMARKING

1. Visible watermarking
2. Invisible watermarking

Visible watermark is an opaque or semi-transparent sub-image or image that is placed on top of another image (that is watermarked) so that is obvious to the viewer. An example: a logo placed by TV networks. Typically, performed in the spatial domain.

A Visible watermark

Invisible watermarks cannot be seen with the naked eye but they can be recovered with an appropriate decoding algorithm. The invisibility is assured by inserting them as visually redundant information (something that human visual system does not perceive): watermarked image after high quality JPEG compression and the extracted watermark.



A Invisible watermark

III. PROBLEM SPECIFICATION

There are numerous watermarking methods till date, which can be classified, as described earlier, according to the method of embedding of data inside the medium. All these methods vary mostly in the prospect of providing robustness against attacks, both intentional and unintentional. Here we present two of the most prevalent approaches, and their detailed analysis with the various benchmarks specified. The two methods are:

1. LSB Modification**:** One of the most basic techniques of embedding data inside a medium. It involves *modification* of the LSB of the pixel with the data to be hidden. Although, this approach is not robust to attacks of most of the kinds, it gives a basic overview of the entire watermarking procedure.
2. Spread-Spectrum Technique: Recent development in this technique has utilized the concept of Spread-Spectrum technique prevalent in Communications. Arguably, one of the most robust technique, here we consider a new non-linear technique of watermarking.

The above two techniques are analysed by using various *distortion metrics* to verify the methods for their robustness. Standard test images like Lenna etc. have been used and the analysis results have been limited to images of Human Faces (or similar type), and the final observations tabulated and a conclusion made.

IV. LSB MODIFICATION TECHNIQUE

A large number of commercial steganographic programs use the Least Significant Bit embedding (LSB) as the method of choice for message hiding in 24-bit, 8-bit color images, and grayscale images. It is commonly believed that changes to the LSBs of colors cannot be detected due to noise that is always present in digital images. In this paper, we describe a new very accurate and reliable method that can detect LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images.

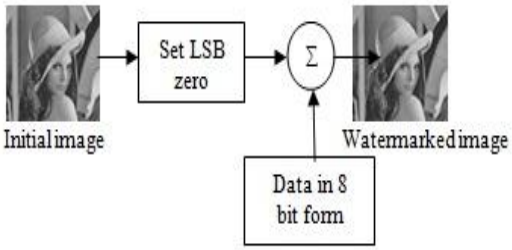


Figure2. LSB Modification Watermarking

V. SPREAD SPECTRUM TECHNIQUE

The definition of spread spectrum may be stated in two parts:

1. It is a means of transmission in which the data sequence occupies a bandwidth in excess of the minimum bandwidth necessary to send it.
2. The spectrum spreading is accomplished *before* transmission through the use of a code that is independent *of* the data sequence. The same code is used in the receiver (operating in synchronism with the transmitter) to de-spread the received signal so that the original data sequence may be recovered.

The spread spectrum technique thus delivers the system the ability to *reject* interference, be it intentional or unintentional. Two main techniques used for spread-spectrum modulation are:

Direct-sequence technique: The data sequence is used to modulate a wide band code, transforming the narrow-band data sequence to a noise like wide-band signal. This signal undergoes a second modulation using a phase-shift keying technique.

Frequency-hop technique*:* changing the carrier by changing the carrier frequency in a pseudo-random manner widens the spectrum of a data modulated carrier.

VI. DISCRETE COSINE TRANSFORM

It is a technique for expressing a waveform as a weighted sum of cosines. Given data A(i), where i is an integer in the range 0 to N-1, the forward DCT (which would be used e.g. by an encoder) is:

$$B(k) = \sum_{i=0}^{N=1} A(i)\cos((\text{pi } k/N)(2i+1)/2)$$

B(k) is defined for all values of the frequency-space variable k, but we only care about integer k in the range 0 to N-1. **The inverse DCT** (which would be used e.g. by a decoder) is**:**

$$AA(i) = \sum_{i=0}^{N=1} B(k)(2\text{-delta}(k\text{-}0))\cos((\text{pi } k/N)(2i+1)/2)$$

Where delta(k) is the Kronecker delta

The main difference between this and a discrete Fourier transform (DFT) is that the DFT traditionally assumes that the data A(i) is periodically continued with a period of N, whereas the DCT assumes that the data is continued with its mirror image, then periodically continued with a period of 2N. Mathematically, this transform pair is exact, i.e. AA(i) == A(i), resulting in lossless coding; only when some of the coefficients are approximated does compression occur.

VII. DISTORTION METRICS

The watermark robustness dependents directly on the embedding strength, which in turn influences the visual degradation of the image. For fair benchmarking and performance evaluation, the visual degradation due to the embedding is an important and unfortunately often neglected issue. Since there is no universal metric, we review in this section the most popular pixel based distortion criteria and introduce one metric, which makes use of the effect in the human visual system (HVS).

VIII. DIFFERENT TYPES OF NOISES

1. Gaussian
2. Localvar
3. Poisson
4. Salt & pepper
5. Speckle

Gaussian noise is a statistical noise that has its probability density function equal to that of the normal distribution , which is also known as Gaussian distribution. It having constant mean and variance. Gaussian noise is most commonly used to yield additive white Gaussian noise.

Localvar noise having Zero-mean Gaussian white noise with an intensity-dependent variance.

Poisson noise arises from poisson processes. It applies to various phenomena of discrete properties whenever the probability of phenomena happening it constant in time or space.

Salt & pepper noise is a form of noise typically seen on images. It represents itself as randomly occurring white and black pixels,

Speckle noise is a granular noise that inherently exists in and degrades the quality of the active radar and synthetic aperture radar (SAR) images.

Speckle noise in conventional radar results from random fluctuation in the return signal from an object that is no bigger than a single image processing element. It increases the mean grey level of a local area.

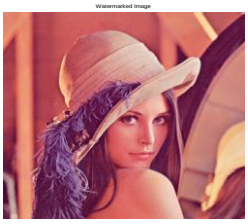
IX. Application Areas

There are many applications for digital watermarking of images, including copyright protection, feature tagging, and secret communications.

1. Copyright Protection: A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property. This is the watermarking scenario where the message is the watermark. The "watermark" can be a relatively complicated structure. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified. Detection of an embedded watermark is performed by a statistical, correlation, or similarity test, or by measuring other quantity characteristic to the watermark in a stego-image. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent surge of interest in digital watermarking and data embedding.
2. Feature Tagging: Captions, annotations, time stamps and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features. In an image database, keywords can be embedded to facilitate search engines. If the image is a frame of a video sequence, timing markers can be embedded in the image for synchronization with audio. The number of times an image has been viewed can be embedded for "pay-preview" application.
3. **Secret Communications**: In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use steganography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers or eavesdroppers.
4. **Ownership assertion**: A rightful owner can retrieve the watermark from his content to prove his ownership.
5. **Fingerprinting**: An owner can embed a watermark into his content that identifies the buyer of the copy (c.f. serial number). If unauthorized copies are found later, the owner can trace the origin of the illegal copies.
6. **Authentication**: The creator of content can embed a *fragile watermark* into the content to provide a proof of authenticity and integrity. Any tampering of the original content destroys the fragile watermark and thus can be detected.

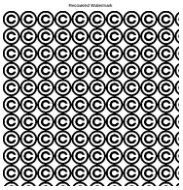
X. RESULT

Watermarked image

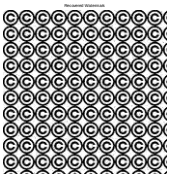


Watermarked and noised image

Recovered watermark



Recovered watermark and noise



XI. CONCLUSION

In this paper, an analysis for image watermarking has been presented.

The analysis embeds the watermark code by LSB modification and DCT of the image, and exploits a model derived from image compression techniques for adapting the watermark strength to the characteristics of the HVS. The performances of the novel algorithm are very good, experimental results, in fact, supported the suitability of DCT watermarking schemes for robustly hiding watermarks into images. In particular, the behavior of the watermark detector with respect to image cropping was surprisingly good. As a matter of fact, DCT schemes do not spread the watermark all over the image, but, the watermarking energy can be kept so high that even a small portion of the image is sufficient to correctly guess the embedded code. As Watermarking becomes more widely used in computing there are issues that need to be resolved. There are a wide variety of different techniques with their own advantages and disadvantages.

REFERENCES

[1] Ingemar J. Cox,Joe Kilian, Tom Leighton, Talal G. Shamoon on "Secure Spread Spectrum Watermarking from Multimedia, IEEE, ICIP' 97, volume 6, Santa Barbara, California, USA, October 1997.

[2] Maryline Charrier, Diego Santa Cruz, and Mathias Larsson, JPEG2000, the Next Millennium Compression Standard for Still Images. In Proceedings of the IEEE, ICMCS '99volume 1,

[3] Mahalingam Ramkumar, Ali N. Akansu, and A. Aydın Alatan. A robust data hiding, Florence Italy, June 1999
scheme for images using DFT. In Proceedings of the 6th IEEE International Conference on Image Processing, ICIP' 99,, Kobe, Japan, October 1999 .

[4] Improved Wavelet-Based Watermarking Through Pixel-Wise Masking Mauro Barni, Member, IEEE, Franco Bartolini, Member, IEEE, and Alessandro Piva, IEEE TRANSACTIONS ON IMAGEPROCESSING, VOL. 10, NO. 5, MAY 2001

[5] Digital Image Watermarking in the wavelet transform domain, Diplomarbeit, Peter Meerwald, Salzburg,am , 11 Janner 2001.

[6] A. G. Bors, "Watermarking Mesh-Based Representationsof 3-D Objects Using Local Moments," IEEE Trans. on Image Processing, vol 15, no., Mar. 2006. © IEEE

[7] Ram Ratan, 'Invisible Messages'

[8] M.KutterandF.A.P.Petitcolas.'AFair Benchmark for Image Watermarking Systems', vol.3657 International Society for Optical Engineering.

[9] Ingemar J. Cox, Joe Kilian, Tom Leighton and Talal Shamoon. 'A Secure, Imperceptable yet Perceptually Salient, Spread Spectrum Watermark for Multimedia',

[10] K.K.Wong,C.H.Tse,K.S.Nag and L.M.Cheng. 'Adaptive Watermarking',IEEE transactions on Consumer lectronics,vol.43,Nov.1997