ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 4 Issue 1 January-February 2016
International Manuscript ID : 23482001V4I101022016-29
(Approved and Registered with Govt. of India)

WATERMARKING - AN EFFECTIVE APPROACH FOR SECURITY AND INTEGRITY

Bhavsar Dharmeshkumar Bhalchandra
Research Scholar
Shri Venkateshwara University
Uttar Pradesh, India

Dr. Parveen Kumar
Professor
Shri Venkateshwara University
Uttar Pradesh, 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,[1] 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 banknote authentication. *This work deals with watermarking in general applied to image processing. The pros and cons of three methods which are used are discussed, which include least significant bit modification(LSB) in the spatial domain and Discrete Cosine Transform(DCT) and wavelet based transform (DWT) in the frequency domain. The algorithms are executed in matlab and in each case the results were obtained for both embedding as well as recovery of the watermark.*

Introduction

The internet has become an indispensable part of todays world and it has led to an expansion of the digital media by leaps and bounds. The risk of piracy is exacerbated by the proliferation

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 4 Issue 1 January-February 2016
International Manuscript ID : 23482001V4I101022016-29
(Approved and Registered with Govt. of India)

of high-capacity digital recording devices. The sudden increase in watermarking interest is most likely due to the increase in concern over copywright protection of content. Watermarking techniques are developed for audio, image and video data. Digital watermarking is a special case of information hiding, where information hiding describes the imperceptible communication of information by embedding it and retrieving it from the other digital data. Additional applications for information hiding are for instance, covert communication (steganography) or the embedding of supplemental information into multimedia data. The latter application is particularly interesting if the embedded information remains receivable even after processing like A/D and D/A conversion. The most important requirements of digital watermarking are:

- Imperceptibility : the watermarked data and the original data should be perceptually indistinguishable.
- Robustness : processing of the watermarked data cannot damage or even destroy the embedded information without rendering the processed data useless, and
- Security : the embedded information can be detected, decoded and/or modified by authorized parties.

Watermarking finds its application in the following areas:

1. Broadcast Monitoring: Watermarking exists within the content itself rather than exploiting a particular segment of the broadcast signal.
2. Owner Identification : Because watermarks can be made both imperceptible and inseparable from the work that contains them, they are likely to be superior to text for owner identification. If users of the work are supplied with watermark detectors, they should be able to identify the owner of a watermarked work, even after the work has been modified in ways that would remove a textual copywright notice.
3. Transaction Tracking : The watermark records one or more transactions that have taken place in the history of the copy of a work in which it is embedded. The owner of the work would place a different watermark in each copy. If the work were subsequently misused the owner would find out who is responsible.
4. Content Authentication: Watermark can yield localized authentication and also examines whether lossy compression has been applied to the work.

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 4 Issue 1 January-February 2016
International Manuscript ID : 23482001V4I101022016-29
(Approved and Registered with Govt. of India)

5. Copy Control : Watermarks are embedded in the content itself, they are present in every representation of the content. If every recording device were fitted with a watermark detector, the devices could be made to prohibit recording whenever a never-copy watermark is detected at its input.
6. Device Control : Copy control falls into a broader category of applications, which we refer to device control.A unique identifier is embedded into printed and distributed images such as magazine advertisements , tickets etc. After the the image is recaptured by a digital camera , the watermark is read by the software on PC and the identifier is used to direct a web browser to an associated web site.

Image watermarking is the process of inserting hidden information in an image by introducing modifications to its pixels with the expectation of minimum perceptual disturbance. Watermarking is robust but still these could be the possible sources of attacks:

- Enhancement: sharpening, contrast, color correction
- Additive and multiplicative noise: Gaussian, uniform, speckle
- Linear filtering: lowpass, highpass, bandpass
- Nonlinear filtering: median filters, rank filters, morphological filters

The more difficult task is providing metrics for perceptibility and robustness. Petitcolas as well as others suggest the scheme listed below in table 1 for the evaluation of perceptibility [14].

Level of Assurance	Criteria
Low	- Peak Signal-to-Noise Ratio (PSNR) - Slightly perceptible but not annoying
Moderate	- Metric Based on perceptual model - Not perceptible using mass market equipment
Moderate High	- Not perceptible in comparison with original under studio conditions
High	- Survives evaluation by large panel of persons under the strictest of conditions.

Table 1 - Summery of Possible Perceptibility Assurance Levels [14]

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 4 Issue 1 January-February 2016
International Manuscript ID : 23482001V4I101022016-29
(Approved and Registered with Govt. of India)

Petitcolas also provides us with a rough set of reliability or robustness metrics, shown below in table 2.

	Level Zero	Low Level	Moderate
Standard JPEG Compression Quality	100 - 90	100 - 75	100 - 50
Color Reduction (GIF)	256	256	16
Cropping	100 - 90%	100 - 75%	100 - 50%
Gamma Correction		0.7-1.2	0.5-1.5
Scaling		$\frac{1}{2} - \frac{3}{2}$	$\frac{1}{3} - 2$
Rotation		+/- 0 - 2 deg.	+/- 0 - 5 deg. 90 deg.
Horizontal Flip		Yes	Yes
Uniform Noise		1-5%	1-15%
Contrast		+/- 0 - 10%	+/- 0 – 25%
Brightness		+/- 0 – 10%	+/- 0 – 25%
Median Filter			3 x 3

Table 2 - Basic Robustness Requirements [14]

Methods:

Least Significant bit Modification:

The most straight-forward method of watermark embedding, would be to embed the watermark into the least-significant-bits of the cover object . Given the extraordinarily high channel capacity of using the entire cover for transmission in this method, a smaller object may be embedded multiple times. Even if most of these are lost due to attacks, a single surviving watermark would be considered a success.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 4 Issue 1 January-February 2016

International Manuscript ID : 23482001V4I101022016-29

(Approved and Registered with Govt. of India)

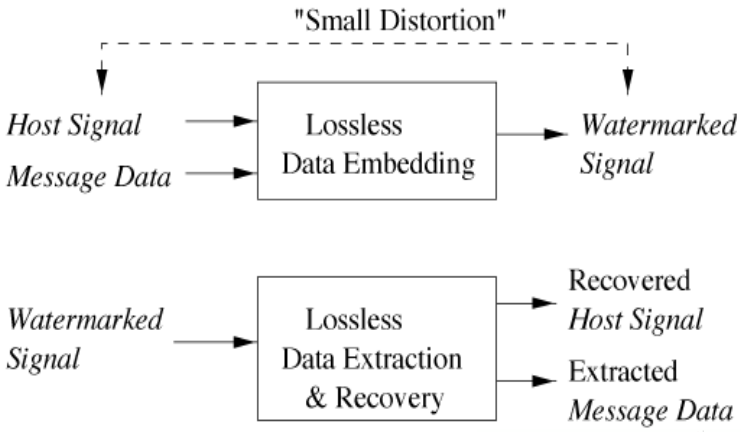

Figure 1

Grid containing 3 pixels of a 24 bit color image using 9 bytes of memory.

00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001

The character A with a binary value 10000001 is inserted in the following grid

00100111	1110100**0**	11001000
0010011**0**	11001000	1110100**0**
11001000	00100111	11101001

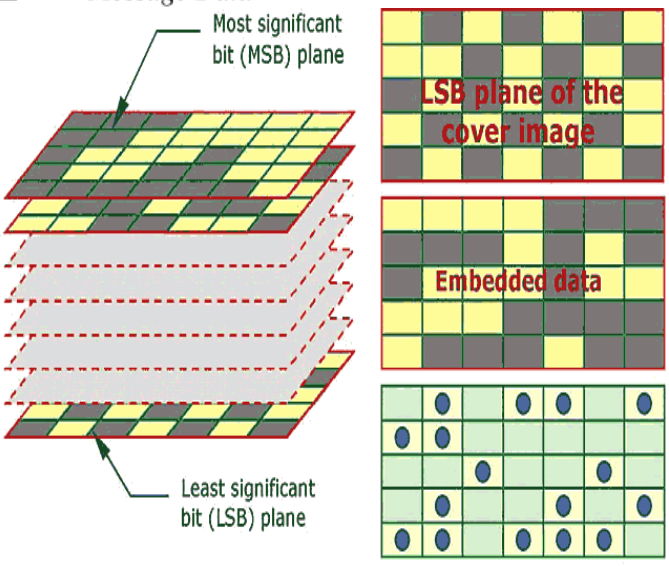

Figure 2

Bit-planes of a grayscale image are sketched on the left with MSB on top. Dark and light boxes represent binary values 0s and 1s, respectively, of the pixels on different bit-planes. The LSB-plane of the cover image on the top right is replaced with the hidden data in the middle, which becomes the LSB-plane of the stego-image. The bottom-right map indicates differences between LSB planes of the cover- and stego-images. Circles represent the flipped bits; with an

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 4 Issue 1 January-February 2016
International Manuscript ID : 23482001V4I101022016-29
(Approved and Registered with Govt. of India)

average of 50% bits in the LSB plane changed, the stego-image is visually identical to the cover.

LSB substitution however despite its simplicity brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression is likely to defeat the watermark. An even better attack would be to simply set the LSB bits of each pixel to one…fully defeating the watermark with negligible impact on the cover object. Furthermore, once the algorithm is discovered, the embedded watermark could be easily modified by an intermediate party.

Frequency Domain Techniques:

An advantage of the spatial techniques discussed above is that they can be easily applied to any image,

Taking these aspects into consideration, working in a frequency domain of some sort becomes very attractive. 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 regardless of subsequent processing (whether they survive this processing however is a different matter entirely). A possible disadvantage of spatial techniques is they do not allow for the exploitation of this subsequent processing in order to increase the robustness of the watermark.

In addition to this, adaptive watermarking techniques are a bit more difficult in the spatial domain. Both the robustness and quality of the watermark could be improved if the properties of the cover image could similarly be exploited. For instance, it is generally preferable to hide watermarking information in noisy regions and edges of images, rather then in smoother regions. The benefit is two-fold; Degradation in smoother regions of an image is more noticeable to the HVS, and becomes a prime target for lossy compression schemes.

image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies).

One such technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies (FM) of an 8x8 DCT block as shown below in figure.

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 4 Issue 1 January-February 2016
International Manuscript ID : 23482001V4I101022016-29
(Approved and Registered with Govt. of India)

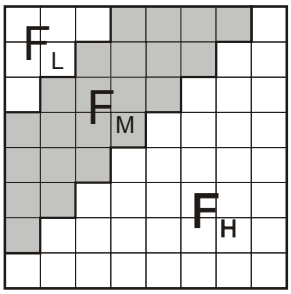

Figure 3

FL is used to denote the lowest frequency components of the block, while FH is used to denote the higher frequency components. FM is chosen as the embedding region as to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image.

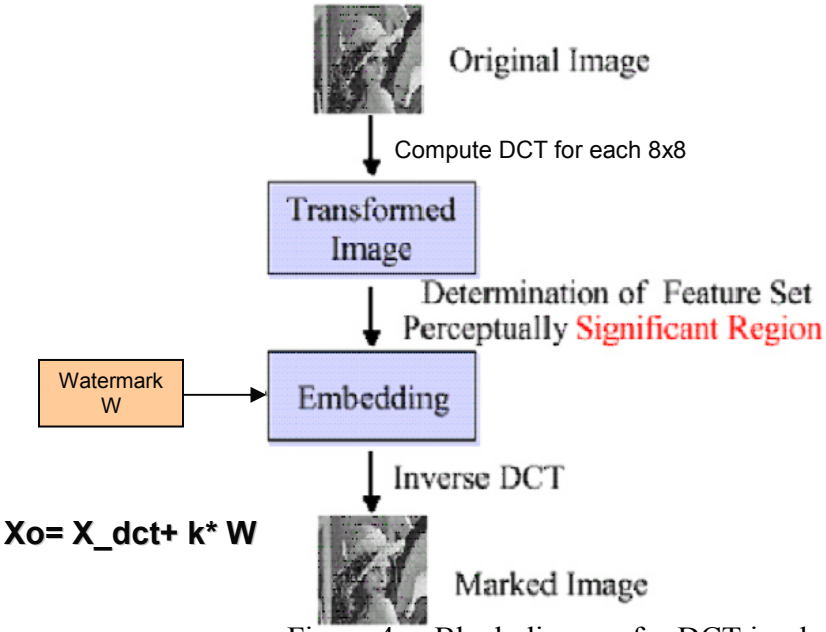

Figure 4 Block diagram for DCT implementation of watermark

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 4 Issue 1 January-February 2016
International Manuscript ID : 23482001V4I101022016-29
(Approved and Registered with Govt. of India)

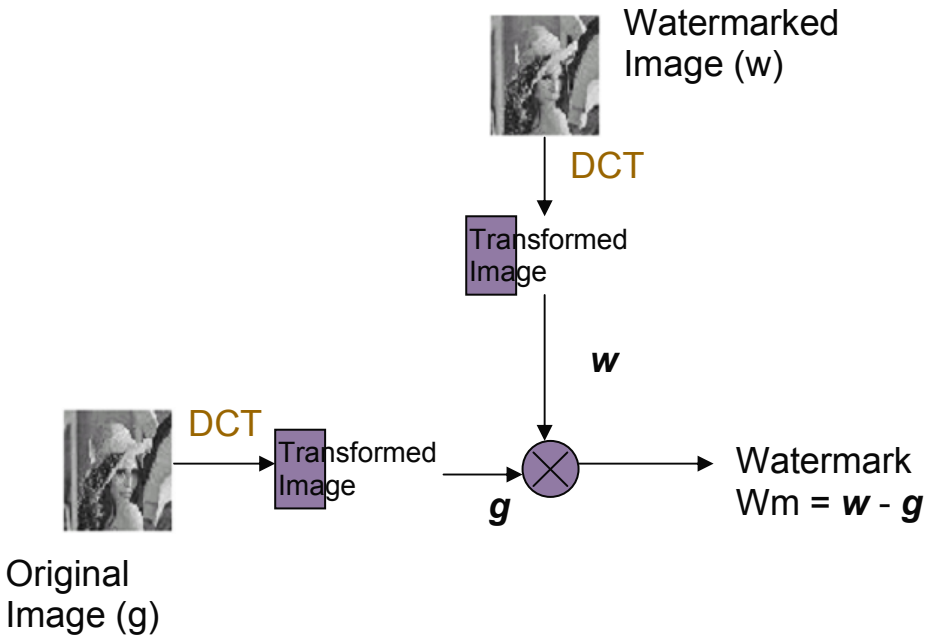

Figure 5 Block Diagram for DCT recovery of watermark.

Wavelet Based Watermarking:

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 computes multiple "scale" wavelet decomposition, as in the 2 scale wavelet transform shown below in figure.

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 4 Issue 1 January-February 2016
International Manuscript ID : 23482001V4I101022016-29
(Approved and Registered with Govt. of India)

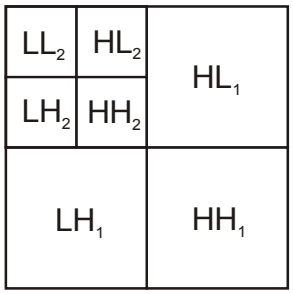

Figure 6 2 scale 2 dimensional DWT

One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the HVS as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high resolution detail bands {LH,HL,HH). Embedding watermarks in these regions allow us to increase the robustness of our watermark, at little to no additional impact on image quality.

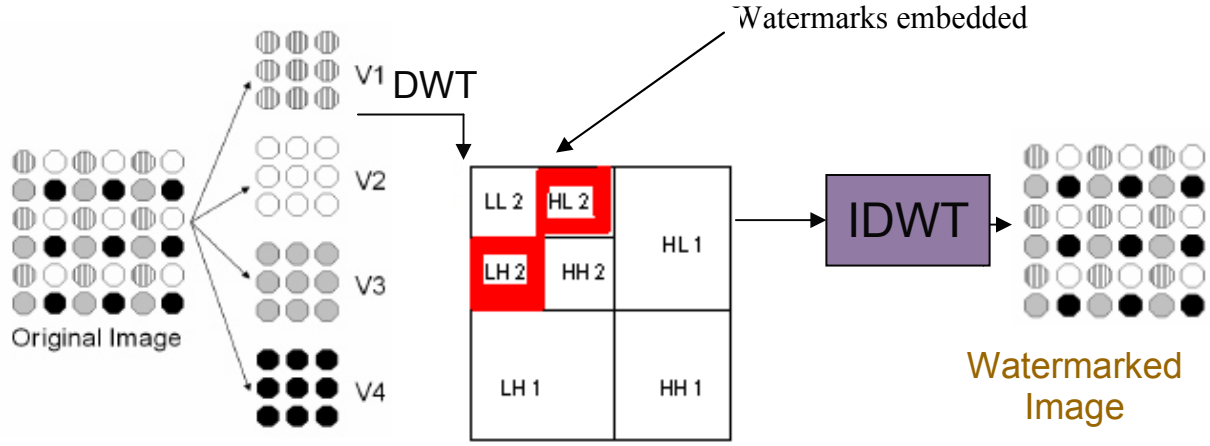

Figure 7 Block diagram showing DWT implementation of watermarking

The image is decomposed into four subimages through subsampling, then they are transformed via DWT to obtain the sets of coefficients Vi[n1,n2]. One pair of coefficients from two different subimages situated in the same DWT domain location is used to insert one watermark sample. The watermark insertion order sequence is that four consecutive numbers in the sequence must be different. When the pair of

ISSN (Online) : 2348 - 2001
International Refereed Journal of Reviews and Research
Volume 4 Issue 1 January-February 2016
International Manuscript ID : 23482001V4I101022016-29
(Approved and Registered with Govt. of India)

coefficients are Vi and Vj, the following operations are performed.

$$V=(Vi+Vj)/2$$

If $abs[(Vi-Vj)/V] < 6a$,

Then $Vi' = V(1 +aW)$,

$Vj'=V(1-aW)$; where positive constant a is the watermark strength control variable which is a ttradeoff between image distortion and detection accuracy.

At the decoder stage similar process is followed. If the recovered watermark is W'[n] and each selected pair of coefficients as Ui and Uj, $U=(Ui+Uj)/2$;

If $(Ui-Uj)/U < 6a$, then

$$W'=(Ui-Uj)/(a*(Ui+Uj).$$

Conclusions:

The project demonstrates the different methods to watermark an image in both spatial domain with the LSB method and in the frequency domain using DCT and DWT. The LSB is not a robust method but the frequency domain techniques are quite resistant to compression and noise. In all these cases the original image is required to extract the watermark. Out of the three methods the DWT method has given better results compared to the others. In future the algorithms are expected to eliminate the need of original image to recover the watermark image and also they should be able to extract watermark from an imagery that has been degraded by several geometric and signal processing methods like cropping, rotation, scale change and translation.

References :

[1] Chang, C.-C., Chuang, J.-C., & Lin, P.-Y. (2013). A grayscale image steganography established upon discrete cosine transformation. [Technical report]. Journal of Digital Data Management, 8(2), 88+.

[2] McBride, B. T., Peterson, G. L., & Gustafson, S. C. (2009). A novel blind method for detecting novel steganography. Digital Investigation, 2(1), 50-70. doi: 10.1016/j.diin.2005.01.003

[3] Min-Jen, T., & Jung, L. (2011, 6-9 Nov. 2013). The quality evaluation of image recovery assault for visible watermarking algorithms. Paper presented at the Visual Communications and Image Processing (VCIP), 2011 IEEE.

[4] Husainy, M. A. F. A. (2009). Image steganography by representing pixels to letters. [Report]. Journal of Computer Science, 5(1), 33+.

[5] Ibrahim, B., Jabri, R., & Zoubi, H. A. (2012). Data concealing: a generic approach. [Technical report]. Journal of Computer Science, 5(12), 933+.

ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 4 Issue 1 January-February 2016

International Manuscript ID : 23482001V4I101022016-29

(Approved and Registered with Govt. of India)

[6] "Steganography: The art of hide data in a plain sight", IEEE, February/March, 2009.

[7] Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhan, "data hiding – A Survey", Proceedings of the IEEE, July, 1999, Vol. 87, No.7.

[8] Arvind Kumar and Km. Pooja "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2012.