Review on Digital Watermarking Techniques

Miss Bhagyashri Dattatray Nikam,
Electronics Department,
Terna Engineering College Nerul Navi,Mumbai

Prof. Mrs. S. B. Gaikwade.
Electronics Department,
Terna Engineering College Nerul Navi Mumbai

Abstract

The massive growth of the world wide web along with the increasing availability of multimedia resources has increased a number of copyright issues. One of the areas that this growth has fueled is that of digital watermarking. Digital watermarking is the general technique of embedding a digital signal in the original file which may be used to verify its authenticity or the identity of its ownership. The approaches to watermarking are diverse and can be broadly classified based on their visibility, robustness and fragility. Their uses are also versatile, as they can be applied to text, images, audio, or video. In this paper, I did study on some of the watermarking algorithms for digital images.

Classification of Watermarking Techniques :

Watermarking techniques can be classified in to two category depending on their visiblity.

***Visible watermarks*: **A visible alteration of the digital image by appending a “stamp” on the image is called a visible watermark. This technique directly maps to that of the pre-digital era where a watermark was printed on the document of choice to impose authenticity. It has stronger robustness, but its applications are limited.

***Invisible watermarks*: **An invisible watermark is based on intensity of embedding watermark. For less intensity watermark better invisiblness can be achieved. So we must select the optimum intensity to embed watermark.Another way of classifying watermarking technique is a factor of its usage : robust, fragile, or semi-fragile, and spatial or spectral watermarks.

***Robust watermarks*: **In Robust Watermarking embedded Watermark can oppose the common edit processing, image processing and lossy compression. It is not destroyed after some attack and It still provide Certification.

***Fragile watermarks*: **These are opposite to robust watermarks. It is more change-sensitive than robust watermarks. They lose their mettle when they are subject even to the smallest changes. We can determine whether the data has been changed according to the state of fragile watermarking.

***Spatial watermarks*: **Watermarks that are applied to the “spatial domain of the image” are said to be spatial watermarks [5].

***Spectral watermarks*: **These watermarks are applied to the “transform coefficients of the image”. [5]The rest of the paper is organized as follow. The ground rules for a good watermark will be laid down in the next section. After describing the various stages of the watermarking process, I will also go over three algorithms for watermarking, and finally analyze the algorithms.

Criteria for a good watermark:

Though watermarks belong to different categories, some of the general characteristics that watermarks must possess are the following [6]:The watermark must be strongly bound to the image and any changes to the watermark must be apparent in the image.

1. Watermark must also be able to withstand changes made to the image. Such changes include modifications and enhancements of images such as size modifications, cropping, lossy compression, to name a few.
2. The watermark must not undermine the visual appeal of the image by its presence (especially for invisible watermarks).
3. Watermark must be indelible and must be able to survive linear or non-linear operations on the image [2].

The following are criteria for a visible watermark: [7]

1. The watermark must be apparent on all kinds of images.
2. The size of the watermark is crucial. The more pervasive the watermark the better so that the watermarked area cannot be modified without tampering with the image itself.
3. The watermark must be fairly easy to implant in the image.

The Watermarking Process:

The watermarking process comprises of the following stages [9]:

1. Embedding stage
2. Extraction phase
3. Distribution stage
4. Decision stage

Embedding stage: In this stage, the image to be watermarked is preprocessed to prime it for embedding. This involves converting the image to the desired transform. This includes the discrete cosine transform (DCT), the discrete Fourier transform (DFT) and the wavelet domains. The watermark to be embedded may be a binary image, a bitstream or a pseudo-random number that adheres to, say, a Gaussian distribution. The watermark is then appended to the desired coefficients (low frequency or intermediate frequency) of the transform, as recommended by Human Visual System (HVS) research. The watermarked image is the output of this process and is obtained by performing an inverse transform on the altered transform coefficients [9].

Distribution stage: The watermarked image obtained above is then distributed through digital channels (on an Internet site). In the process, this may have undergone one of several mappings, such as compression, image manipulations that downsize the image, enhancements such as rotation, to name a few. Peter Meerwald [9] refers to the above as “coincidental attack”. Any of the above may put the watermarking scheme to test, as we will see in the ensuing section. In addition, malicious attacks also are possible in this stage to battle with the watermark. These are referred to in Meerwald's work [9] as "hostile attacks".

Extraction stage: In this stage, an attempt is made to regain the watermark or signature from the distributed watermarked image. This stage may need a private key or a shared public key, in combination with the original image, or just the watermarked image [9].

Decision stage: In this stage, the extracted watermark is compared with the original watermark to test for any discrepancies that might have set in during distribution. A common way of doing this is by computing the Hamming distance [9].

$$HD = \frac{(W^{mod}. W)}{||W^{mod}||.||W||}$$

where both the numerator and denominator are dot products.

HD obtained above is compared to a threshold, T, to determine how close W^{mod} is to W.

Techniques used for digital watermarking:

Hash Functions as fragile watermarks:

According to Wolfgang and Delp[3], hash functions can be used as fragile watermarks. One of the methods they have used as watermarks is the block-based hash function (BBHF) [3]. The hash is computed on the width and height of the image block. Specifically, X_b is the width of the block and Y_b is the height of the block and $X_b * Y_b$ is the hash function. The hash values of every block of the image are stored. In order to test the sanctity of an image, the stored hash values are compared to the hash values of the image whose sanctity is to be tested. If the hash values do not correspond to each other, then the block which houses the discrepancy is the one that has been altered (see figure 1 in the appendix).

Variable-Watermark Two-Dimensional Algorithm (VW2D) [3]

Wolfgang and Delp have developed this algorithm for image authentication. Both the watermark and the watermarked image are used here to authenticate the image. A pseudorandom binary sequence is the watermark and this sequence is superimposed on the original image in blocks. This can be elucidated as follows: Let WI be the watermarked image, W be the watermark and X be the original image. Then WI_b is a block of the watermarked image, W_b is a block of the watermark and X_b is a block of the original image. The watermarked image is generated as follows [3]:

$$WI = WI_{b1} + WI_{b2} + \ldots + WI_{bn}$$

And each watermarked image block is generated as follows:

$$WI_{bi} = X_{bi} + W_{bi} \quad \text{(where I = 1 to n)}$$

Checking to see if a watermark resides in an image (Test) is done as follows:

$$\triangle_{bi} = WI_{bi} . W_{bi} - Test_{bi} . W_{bi}$$

A threshold value can be chosen to authenticate the test image. The threshold is compared with the delta value computed above. The choice of the threshold value can determine the extent of changes that are tolerated to the watermarked image. The spectrum of scenarios that can be tested range gradually from unchanged to highly manipulated. Such a choice also gives the users of this algorithm some leeway in choosing the strictness with which manipulations are caught. The effect of choosing different threshold values can be seen in the images in the Appendix (Figures 2,3,4,5).

Human Visual System (HVS):

In order to develop good watermarking algorithms, characteristics of the human visual system have been extensively studied. The nuances of visual perception have given scientists an insight into modeling watermarks that do not interfere with the host image. Wolfgang, Delp and Podilchuk [2] have listed some of the characteristics of the human visual system by the following 3 criteria, as given in Wolfgang et al's paper [2]:

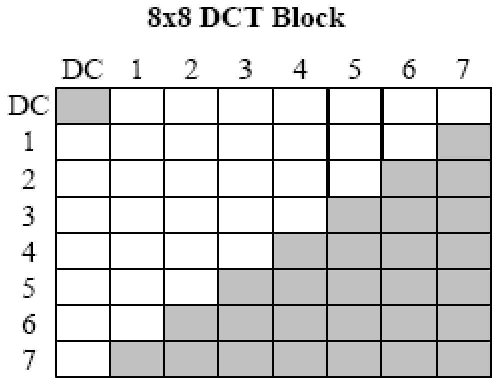
1. Sensitivity to frequency: the HVS is more sensitive to higher frequencies than to lower frequencies. [2]

2.Contrast masking: This refers to how one signal influences the expression of another signal. Presence of two signals in the same frequency enhances this property [2].While the above two algorithms have been applied to the spatial domain of the image, watermarking algorithms that tap into various transforms became popular, thanks to their robustness and quality. Some of the transforms that are used for this purpose include the discrete cosine transform (DCT), discrete Fourier transform (DFT) and the wavelet domains. These techniques combined with studies on the human visual system have allowed for the development of good watermarking techniques.A very popular compression technology for still images is JPEG [2]. Compression in JPEG occurs as follows. The still image to be compressed is passed through a coder, which transforms the image by ripping it into distinct blocks of 8*8 pixels. A DCT is applied on the thus obtained distinct blocks.

A Semi-Fragile Watermark in the DCT domain –Lin's algorithm:

Lin et. al [1] have developed a semi-fragile watermark in the DCT domain.

Watermark: The watermark is given by "pseudo-random zero-mean, unit variance Gaussian distributed numbers"[1].



	DC	1	2	3	4	5	6	7
DC	▨							
1								▨
2							▨	▨
3						▨	▨	▨
4					▨	▨	▨	▨
5				▨	▨	▨	▨	▨
6			▨	▨	▨	▨	▨	▨
7		▨	▨	▨	▨	▨	▨	▨

Figure 1: watermarking process using the DCT domain. The clear blocks are marked coefficients while the grey blocks are unmarked coefficients. Figure obtained from

ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei00-water/paper.pdf
[1]

Embedding stage: Watermark is embedded in every 8*8 DCT block. Though each block has a different watermark, the watermark is embedded on the same indices of each block. The DC coefficient and some other coefficients including the high frequency AC coefficients of the block are not marked. The inverse DCT is constructed to produce the watermark W.[1]

WI= O + strength (W),Where, WI is the watermarked image, O is the original image, and strength is the strength of the watermark.

Detection stage: Detection is done by comparing blocks with corresponding blocks to localize any changes. A threshold is compared to the test value computed for each of the blocks to figure out if a block has been modified. The algorithm described in Lin's paper is discussed below.[1]

Let B(x,y) be an arbitrary block.

Col-diff (Block(x,y)) = Block(x,y) – Block(x+1,y) for x in { 1,2,…blocksize –1)

Or 0 if x = blocksize

Row-diff(Block(x,y))= Block(x,y) – Block(x,y+1) for y in { 1,2,…blocksize –1)

Or 0 if y = blocksize

T is computed as a single matrix obtained by concatenating col-diff anf row-diff of the test image block and water-block is the corresponding matrix for the watermarked image.

T = [Col-diff(T(x,y)) Row-diff(T(x,y))]

W = [Col-diff(W(x,y)) Row-diff(W(x,y))]

Since we need to obtain a dot product, the matrix T and W above are permuted to obtain a vector. The permutation function, F, should be uniform for both the matrices.

F(T) =vector(T)

W(T)=vector(T)

The test statistic, S, can be computed as follows:

S = (T.W) / sqrt((T.T)(W.W))

Comparing the blocks can be done as follows. An appropriate threshold, T, is chosen and compared with the test statistic.

S >= T => block unaltered

S < T => block altered

Evaluation of algorithms:

The hash algorithm and the VW2D algorithms were used in the spatial domain while Lin's algorithm utilized the DCT domain. The hash algorithm is the least tolerant to changes to images, while both VW2D and Lin's algorithm offered some resilience to change in the form of a tolerance level that could be assigned for comparisons. However, while both VW2D and Lin's algorithm can handle lossy compression that JPEG doles out to images, Lin's algorithm also made use of the HVS perception in its algorithm by only making changes to the low frequency coefficients. Since JPEG compression is done using the DCT transform, Lin's algorithm is the best bet for JPEG images. Using any of the above algorithms will reflect changes made to the watermarked images, although to different extents. The watermarks themselves are not too difficult to embed and hence can be embedded easily. An appropriate watermarking process can therefore be chosen, based on the purpose and level of protection required.

Conclusion:

Watermarking is a vast field and a lot of research is going on in this area. Digital watermarking together will definitely provide copyright protection for images. Depending on the given requirements and the level of security required, an appropriate watermarking algorithm can be chosen.

References:

1. E. T. Lin, C. I. Podilchuk, and E. J. Delp, "Detection of Image Alterations Using Semi-Fragile Watermarks," *Proceedings of the SPIE International Conference on Security and Watermarking of Multimedia Contents II,* Vol. 3971, January 23 - 28, 2000, San Jose, CA.
2. R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual Watermarks for Digital Images and Video," *Proceedings of the IEEE,* Vol. 87, No. 7, July 1999, pp. 1108-1126.
3. R. B. Wolfgang and E. J. Delp, "Fragile Watermarking Using the VW2D Watermark," *Proceedings of the SPIE/IS&T International Conference on Security and Watermarking of Multimedia Contents,* vol. 3657, January 25 - 27, 1999, San Jose, CA, pp. 204-213.
4. E. T. Lin and E. J. Delp, "A Review of Fragile Image Watermarks," *Proceedings of the Multimedia and Security Workshop (ACM Multimedia '99) Multimedia Contents,* October 1999, Orlando, pp. 25-29.
5. http://www.ece.purdue.edu/~ace/water2/digwmk.html
6. http://www.acm.org/~hlb/publications/dig_wtr/dig_watr.html
7. http://www.cs.unt.edu/~smohanty/research/ConfPapers/2002/MohantyICME2000.pdf
8. Peter Meerwald and Andreas Uhl, "Digital Watermarking in the Wavelet Transform Domain" , January 2001

Appendix:

The following images are obtained from Dr.Delp's Website at

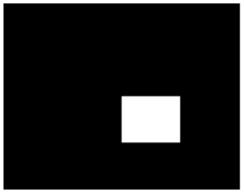


Figure 1:test image for a modified image using BBHF from ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei99-hash/paper.pdf [3]

Figure 2: Original image(before watermarking) .Figure obtained from from ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei99-hash/paper.pdf [3]

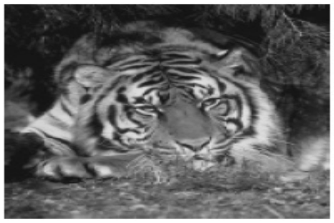


Figure 3: Watermarked image using the VW2D algorithm.
ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei99-hash/paper.pdf
[3]

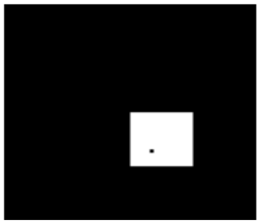


Figure 4 :test image for a modified image using VW2D with a threshold T =0 from
ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei99-hash/paper.pdf [3]

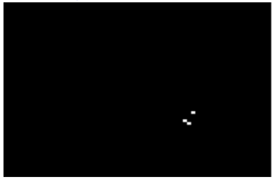


Figure 5:test image for a modified image using VW2D with a threshold T=200 from
ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei99-hash/paper.pdf [3]

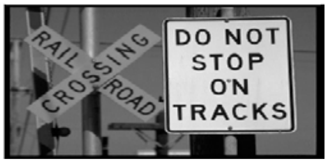


Figure 6: Original image prior to watermarking. Figure obtained from ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei00-water/paper.pdf [1]

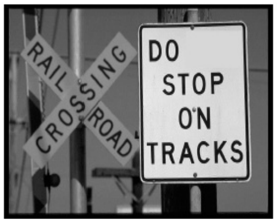


Figure 7: Modified watermarked image (watermarking done using Lin’s algorithm).
ftp://skynet.ecn.purdue.edu/pub/dist/delp/ei00-water/paper.pdf
[1]