Study on Digital Watermarking

Mr .Kunal D. Megha [*], *Associate Prof. S. M. Shah*[#]

** C.S.E. Department, Government Engineering College, Sector-28, Gandhinagar, Gujarat, India*

 # C.S.E. Department, Government Engineering College, Sector-28, Gandhinagar, Gujarat, India

Abstract

Digital Watermarking is the technique used by researchers to hide user defined information along with important information that may be visible or invisible depending upon the requirements of the user. Now Digital watermarking is concerned with the ownership of the information. Absence of Digital Watermark in the information results in loss of revenue. The Digital Watermark packed with the information should be inseparable. This paper will present here the Surveying of digital watermarking.

Keywords: Watermarking, Spatial Domain technology, Discrete Cosine transform (DCT), Discrete Wave late transform (DWT) and Frequency Domain technology.

I. Introduction

Digital Watermarking is to embed a hidden watermark message into a hot object such that the hidden message is inseparable. Earlier watermarking was applied to text only [1]. Now days watermarking is applied to all types of media. Digital watermarking is applied to video also to stop piracy which results in loss of revenue. There should be no perceptible difference between the watermarked and original signal and the watermark should be difficult to remove or alter without damaging the host object. Digital watermarking technology is an emerging field in computer science, cryptography, signal processing and communications.

Digital Watermarking is intended by its developers as the solution to the need to provide value added protection on top of data encryption and scrambling for content protection [2] [3]. Like other technology under development, digital watermarking raises a number of essential questions as follows:

1. What is it?
2. How can a digital watermark be inserted or detected?
3. How robust does it need to be?
4. Why and when are digital watermarks necessary?
5. What can watermarks achieve or fail to achieve?
6. How should digital watermarks be used?
7. How might they be abused?
8. How can we evaluate the technology?
9. How useful are they, which are, what can they do for content protection in addition to or in conjunction with current copyright laws or the legal and judicial means used to resolve copyright grievances?
10. What are the business opportunities?
11. What roles can digital watermarking play in the content protection infrastructure?
12. And many more ...

II. General Framework of Digital Watermarking

Watermarking is the process that embeds data called a watermark or digital signature or tag or label into a multimedia object such that watermark can be detected or extracted later to make an assertion about the object [4]. The object may be an image or audio or video. A simple example of a digital watermark

would be a visible"seal" placed over an image to identify the copyright. However the watermark might contain additional information including the identity of the purchaser of a particular copy of the material.

In general, any watermarking scheme (algorithm) consists of three parts.

- The watermark.
- The encoder (insertion algorithm).
- The decoder and comparator (verification or extraction or detection algorithm).

Each owner has a unique watermark or an owner can also put different watermarks in different objects the marking algorithm incorporates the watermark into the object. The verification algorithm authenticates the object determining both the owner and the integrity of the object.

A) *Encoding Process: -* [4]

Let us denote an image by *I*, a signature by S = S1, S2, and watermarked image by *I'* E is an encoder function, it takes an image *I* and a Signature S, and it generates a new image which is called watermarked image *I*. Mathematically,

E (*I*, S) = *I'* (1)

It should be noted that the signature S may be dependent on image *I*. In such cases, the encoding process described by Eqn. 1 still holds. Following figure illustrates the encoding process.

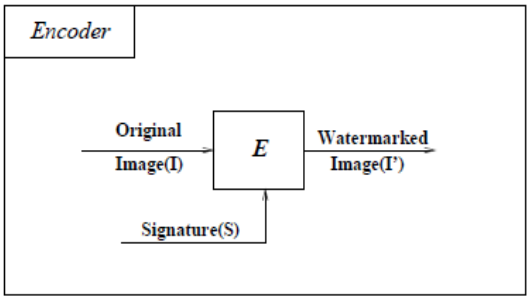

Figure-1: Encoder

B) *Decoding Process: - [4]*

A decoder function D takes an image J (J can be a watermarked or un-watermarked image, and possibly corrupted) whose ownership is to be determined and recovers a signature S' from the image. In this process an additional image *I* can also be included which is often the original and un-watermarked version of J. This is due to the fact that some encoding schemes may make use of the original images in the watermarking process to provide extra robustness against intentional and unintentional corruption of pixels.

Mathematically,

D (J, *I*) = S' (2)

The extracted signature S' will then be compared with the owner signature sequence by a comparator function and a binary output decision generated. It is 1 if there is match and 0 otherwise, which can be represented as follows.

$$C_\delta(S', S) = \begin{cases} 1, & c \le \delta \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

Where C is the correlator,

$$x = C_\delta(S', S).$$

C is the correlation of two signatures and 0 is certain threshold. Without loss of generality, watermarking scheme can be treated as a three-tupple,

$$(E, D, C_\delta).$$

Following figures demonstrate the decoder and the comparator.

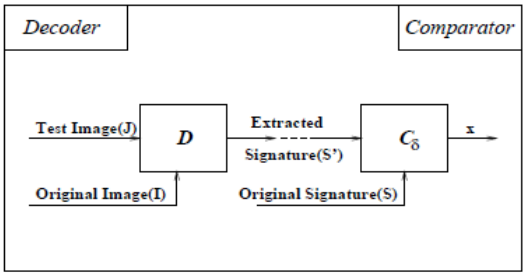

Figure-2: Decoder Process

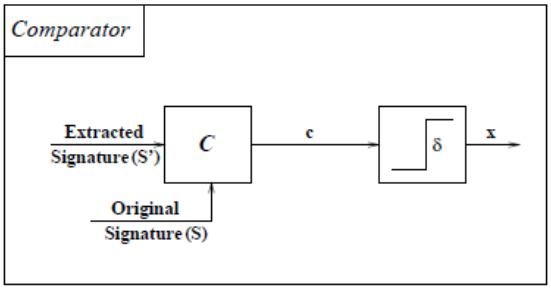

Figure-3: Comparator

A watermark must be detectable or extractable to be useful. Depending on the way the watermark is

inserted and depending on the nature of the watermarking algorithm, the method used can involve very distinct approaches. In some watermarking schemes, a watermark can be extracted in its exact form, a procedure we call watermark extraction. In other cases, we can detect only whether a specific given watermarking signal is present in an image, a procedure we call watermark detection. It should be noted that watermark extraction can prove ownership whereas watermark detection can only verify ownership.

C) Types of Digital Watermarking:-

1) Visible watermarks: -

They designed to be easily perceived by the viewer, and clearly identify the owner; the watermark must not detract from the image content itself, however [5]. Most research currently focuses on invisible watermarks, which are imperceptible under normal viewing conditions.

2) Fragile watermarks: -

A watermark may be fragile, semi-fragile or robust. Fragile watermarks are designed to be distorted or "broken" under the slightest changes to the image. Semi-fragile watermarks are designed to break under all changes that exceed a user-specified threshold. (A threshold of zero would form a fragile watermark.) Robust watermarks withstand moderate to severe signal processing attacks (compression, rescaling, etc.) on an image.

3) Spatial watermarks: -

They are constructed in the image spatial domain, and embedded directly into an image's pixel data. Spectral (or transform-based) watermarks are incorporated into an image's transform coefficients (DCT, Wavelet).

4) Image-adaptive watermarks: -

They are usually transform-based, and very robust. They locally adapt the strength of the watermark to the image content through perceptual models for human vision. These models originally developed for image compression.

5) Blind watermarking: -

These techniques can perform verification of the mark without use of the original image. Other techniques rely on the original to detect the watermark. Many applications require blind schemes; these techniques are often less robust than non-blind algorithms.

D) Application of Digital Watermarking:-

The applications are broadcast monitoring, content authentication and transaction tracking.

1) Broadcast Monitoring: -

Consider a broadcasting studio which plays advertisements for various companies [5]. How can the company know for sure that the studio did actually play the advertisement on the appointed time? One way is to pay someone to watch the studio's broadcast. This is not a feasible solution for a big company that wants hundreds of advertisements broadcast from different studios in a day. Another option for the company is to have all its advertisements watermarked. This way a computer can be set up to scan all TV broadcasting and try to detect the company's watermark. This way the company can tell if their advertisement was broadcast.

A sophisticated watermarking algorithm is not needed in this case because the broadcast signals will only go through natural signal processing. It can be fairly certain that no malicious attacks will be used to remove the watermark.

2) Content Authentication: -

There are circumstances when the artist or composer of a media will want the ability to determine if their work has been altered and, if the work has been altered, how the work was altered. In this way the author of the work can track any misuse of their works. Alteration of media can be determined by first embedding the media with a fragile watermark. A fragile watermark by design will degrade or change as the media is edited. Upon detection of the degraded or changed watermark one can determine that the work has been edited. Also if the fragile watermark is sophisticated enough that the change it goes through is constant under different editing techniques, it can be determined what editing technique was applied to the media.

3) Transaction Tracking: -

The artist or composer of work might wish to sell copies of their work to the public. As copies are sold more and more pirated versions of the work will be created and sold. Pirated copies must be tracked and destroyed. In order to prevent piracy, the artist must track his works. Placing a unique watermark on each copy that is sold can do this. If a pirated copy is detected in the market, the pirated work can be scanned to see what watermark is on it. This way the original copy from which the pirated copies are being

created can be tracked. Thus all sources of pirated copies can be eliminated.

In this type of system the watermark must be very sophisticated and robust. It can be guaranteed that pirates will send the work through malicious attacks in an attempt to remove the watermark.

E) Properties of Digital Watermarking:-

Watermarks have three main properties: fidelity, robustness, and detection error. These properties determine the effectiveness of the watermarks.

1) Fidelity: -
Fidelity refers to the perceptual similarity between the original and watermarked work [5]. A good watermarking algorithm will ensure that the viewer sees no difference between the original and watermarked image.

2) Robustness: -
Robustness refers to the ability of the watermark to survive attacks on the watermarked image. Watermark should be robust enough to survive attacks such as JPEG compression, cropping, scaling etc.

3) Detection Error: -
Detection error is measured in two ways: false negatives and false positives. False negative is when the detector algorithm detects no watermark when there is a watermark present. False positive is when the detector algorithm detects a watermark when there is no watermark present. The detector algorithm should be able to prevent these types of errors.

III. Digital Watermarking Techniques

A) Spatial Domain Technology: - [6]

Spatial-domain technologies refer to those embedding watermarks by directly changing pixel values of host images. Some common spatial-domain algorithms include Least Significant Bit (LSB) Modification, Patchwork, Texture Block Coding, etc. The most serious drawback of spatial-domain technologies is limited robustness.

The LSB is the most straight-forward method of watermark embedding. 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.

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, which 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.

B) Frequency Domain technology: - [6]

Compared to spatial-domain watermark, watermark in frequency domain is more robust and compatible to popular image compression standards. Thus frequency-domain watermarking obtains much more attention. To embed a watermark, a frequency transformation is applied to the host data. Then, modifications are made to the transform coefficients. Possible frequency image transformations include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and others.

The middle range frequency DCT coefficients are then modified, using either a linear DCT constraint or a circular DCT detection region. A DCT domain watermarking technique based on the frequency masking of DCT blocks was introduced by Swanson. Cox developed the first frequency-domain watermarking scheme. After that a lot of watermarking algorithms in frequency domain have been proposed.

Figure 4 and Figure 5 illustrate the watermark embedding and detection /extraction in frequency domain respectively:

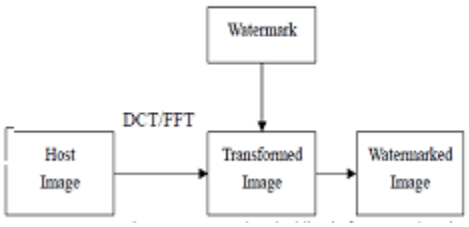

Figure-4: Watermark embedding in frequency domain

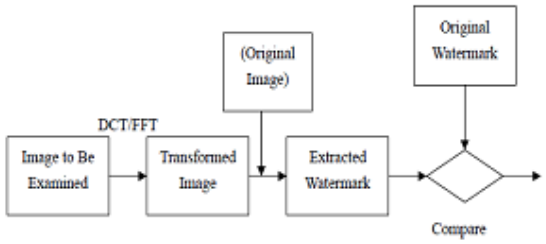

Figure-5: Watermark detection/extraction in frequency

One major reason why frequency domain watermarking schemes are attractive is their compatibility with existing image compression standards, in particular, the JPEG standard. The compatibility ensures those schemes a good performance when the watermarked image is subject to lossy compression, which is one of the most common image processing methods today. In consequence, those schemes become particularly useful in practical applications on the Internet.

A widely accepted point now is the frequency-domain watermark should be embedded into the mid-band of the transformed host image. Watermarks in high frequency band tend to have less influence on the quality of original image, while watermarks in low band will achieve a better robustness (since a large portion of high frequency components may be quantized to zero under JPEG compression, as shown in figure 6). And the mid-bind scheme is right a tradeoffs between the imperceptibility and robustness.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	69	56
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

Figure-6: JPEG quantization table for intensity (left) & hue (right).

C) Discrete Cosine Transform (DCT) techniques: - [7]

With the character of discrete Fourier transform (DFT), discrete cosine transform (DCT) turn over the image edge to make the image transformed into the form of even function. It's one of the most common linear transformations in digital signal process technology. Two dimensional discrete cosine transform (2D-DCT) is defined as

$$F(jk)=a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}f(mn)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad (4)$$

The corresponding inverse transformation (Whether 2DIDCT) is defined as

$$f(mn)=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}a(j)a(k)F(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right] \quad (5)$$

The 2D-DCT can not only concentrate the main information of original image into the smallest low-frequency coefficient, but also it can cause the image blocking effect being the smallest, which can realize the good compromise between the information centralizing and the computing complication. So it obtains the wide spreading application in the compression coding.

D) Discrete Wavelet Transform (DWT) techniques: - [7]

Wavelet transform is a time domain localized analysis method with the window's size fixed and forms convertible. There is quite good time differentiated rate in high frequency part of signals DWT transformed. Also there is quite good frequency differentiated rate in its low frequency part. It can distill the information from signal effectively.

The basic idea of discrete wavelet transform (DWT) in image process is to multi-differentiated decompose the image into sub-image of different spatial domain and independent frequency district [8][9]. Then transform the coefficient of sub-image. After the original image has been DWT transformed, it is decomposed into 4 frequency districts which is one low-frequency district(LL) and three high-frequency districts(LH,HL,HH).

If the information of low-frequency district is DWT transformed, the sub-level frequency district information will be obtained. A two-dimensional image after three-times DWT decomposed can be shown as Fig.7. Where, L represents low-pass filter, H represents high-pass filter. An original image can be decomposed of frequency districts of HL1, LH1,

and HH1. The low-frequency district information also can be decomposed into sub-level frequency district information of LL2, HL2, LH2 and HH2. By doing this the original image can be decomposed for n level wavelet transformation.

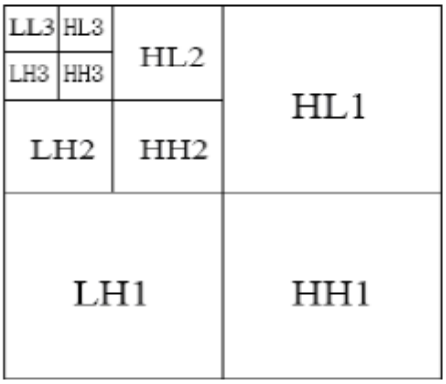

Figure-7: Sketch Map of Image DWT Decomposed

The information of low frequency district is an image close to the original image. Most signal information of original image is in this frequency district. The frequency districts of LH, HL and HH respectively represents the level detail, the upright detail and the diagonal detail of the original image.

According to the character of HVS, human eyes are sensitive to the change of smooth district of image, but not sensitive to the tiny change of edge, profile and streak. Therefore, it's hard to conscious that putting the watermarking signal into the big amplitude coefficient of high-frequency band of the image DWT transformed then it can carry more watermarking signal and has good concealing effect.

IV. Attacks on Watermarks

A watermarked image is likely to be subjected to certain manipulations, some intentional such as compression and transmission noise and some intentional such as cropping, filtering, etc. They are summarized in Fig.8.

A) Lossy Compression: -

Many compression schemes like JPEG and MPEG can potentially degrade the data's quality through irretrievable loss of data [4].

B) Geometric Distortions: -

Geometric distortions are specific to images videos and include such operations as rotation, translation, scaling and cropping.

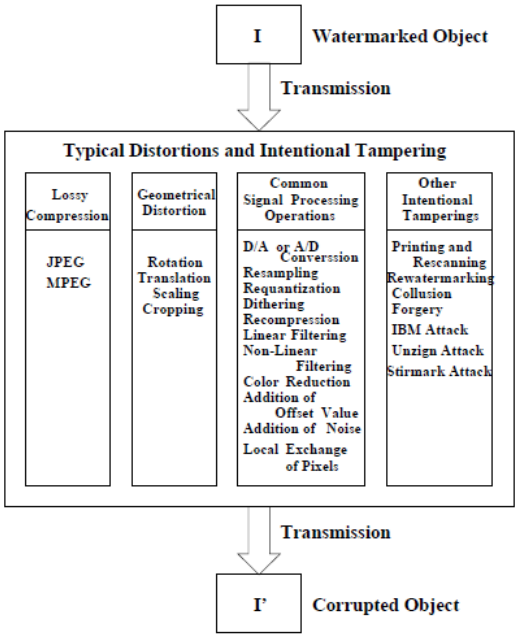

Figure-8: Attacks on Watermarks

C) Common Signal Processing Operations:

They include the followings:

1. D/A conversion
2. A/D conversion
3. Resampling
4. Requantization
5. Dithering distortion
6. Recompression
7. Linear filtering such as high pass and low pass filtering
8. Non-linear filtering such as median filtering
9. Color reduction
10. Addition of a constant offset to the pixel values
11. Addition of Gaussian and Non Gaussian noise
12. Local exchange of pixels

D) Other intentional attacks:-

1. Printing and Rescanning
2. Watermarking of watermarked image (rewatermarking)
3. Collusion: A number of authorized recipients of the image should not be able to come together (collude) and like the differently watermarked copies to generate an un-watermarked copy of the image (by averaging all the watermarked images).

4. Forgery: A number of authorized recipients of the image should not be able to collude to form a copy of watermarked image with the valid embedded watermark of a person not in the group with an intention of framing a 3rd party.
5. IBM attack [10, 11]: It should not be possible to produce a fake original that also performs as well as the original and also results in the extraction of the watermark as claimed by the holder of the fake original.
6. The Unsigned and Stir mark have shown remarkable success in removing data embedded by commercially available programs.

V. Future Work

The watermarking research is progressing very fast and numerous researchers from various fields are focusing to develop some workable scheme. Different companies also working to get commercial products.

In the Future Work, Our aim of proposed research work is to design an algorithm to hide watermark image into original image using Discrete Cosine Transform and Discrete Wavelet Transform Which is robust against all the attacks and analyze the results for the same.

VI. References

[1] Sarabjeet Singh, "Digital Watermarking Trends" International Journal of Research in Computer science.

[2] I. J. Cox, M. L. Miller and J. A. Bloom, "Digital Watermarking", Morgan Kaufman Publishers, 2002.

[3] P. Siva, "Effectiveness of Still Image Digital Watermarking Algorithms", University of Waterloo: Work Term Report, 2002.

[4] Saraju P. Mohnty, "Digital Watermarking: A tutorial review", Dept of Computer Science and Engineering, University of South Florida.

[5] P. Siva, "Effectiveness of Still Image Digital Watermarking Algorithms", University of Waterloo: Work Term Report, 2002.

[6] Lin Liu, "A Survey of Digital Watermarking technologies"

[7] Mei Jiansheng and Li Sukang, "A Digital Watermarking Algorithm based on DCT and DWT", International Symposium on Web Information System and Application ISBN 978-952.

[8] GhoutiL, BouridaneA and Ibrahim MK, "Digital image watermarking using balanced multi wavelets" , IEEE Transactions on Signal Processing, 54(4), pp. 1519-1536, 2006.

[9] Reddy AA, Chatterji BN, "A new wavelet based logo watermarking scheme", Conf. Pattern Recognition letters, 26(7), pp. 1019-1027, 2005.

[10] S.Craver,"Can Invisible Watermarks Resolve Rightful Ownership?" IBM Research Report, RC205209, July25 1996.

[11] S. Craver,"Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks and Implications", IEEE Journal, On Selected Areas in Communications, Vol.16, No.4, May 1998, pp.573-586

[12] http://www.digital-watermark.com

[13] http://www.digimarc.com

[14] http://www.altern.org/watermark

[15] http://www.cl.cam.ac.uk/μ fapp2/watermarking

[16] http://nif.www.media.mit.edu/DataHiding

[17] http://www.intertrust.com