# A Quick Glance at Digital Watermarking

**Bangxi Yu**, bangxiyu@wustl.edu (A project report written under the guidance of Prof. Raj Jain)

Download 


## Abstract

In this survey paper, we give all-around view of digital watermarking. With the rapid development of network and digital technology, security of digital contents becomes a serious problem. Digital watermarking can provide an effective security protection to digital contents. In this paper we start from some basic knowledge about digital watermarking. Then we go deeply with three aspects: algorithm, application and attack. In each aspect, we introduce some traditional instances and some novel instances.

## Keywords

Digital watermarking, Robust, DWT, DCT, DHT, Protection, Attack, Security.

## Table of Contents



## 1 Introduction

Watermarking is an embedded image or pattern in paper, people can view it by transmitted or reflected light. Watermarking is often used as security features of banknotes, passports, postage stamps and other documents. Similarly, digital watermarking is some embedding in formation in a digital signal. It is used to verify the digital signal¡¯s authenticity or the identity of its owners. Common medium on digital watermarking

is audio, picture, or video. Several different digital watermarks can be embedding in one signal at the same time, and if the signal is copied, then the information on it will also be copied and carried in the copy.

Now days, technology is developing more and more fast, it is playing an important role in people¡¯s life and work. With the rapid development of network and digital technology, we widely use the Internet and digital signal to transmit information.[Zhou02] Digital watermarking is used for a wide range of applications, such as: copyright protection, source tracking, broadcast monitoring, covert communication, bills security and authenticity identification.

Digital watermarking is not a novel technology, there are some traditional algorithms and applications, but with the emergence of new digital signal, application and attack, corresponding digital watermarking will appear.

I introduce some rudimentary knowledge of digital watermarking (in section 2), it can help people better understand the content of other sections. In section 3-5, I discuss algorithm, application and attack in digital watermarking, in all these three sections, I come up with two points: traditional and novel. In section 6, I try to assume some directions of developments of digital watermarking.

# 2. Background

In this section, I use three subsections to briefly introduce some basic knowledge of digital watermarking from three aspects which may be useful in the follow sections. [Wikipedia 15]

## 2.1. Visible/invisible digital watermarking

Visible and invisible are the two basic types of digital watermarking, and every digital watermark can be considered as either visible or invisible.

Visible digital watermarking is a way by which anybody can put visible information in digital signal, the information is often a logo, which identifies the owner of the digital signal. For example, a television broadcaster usually adds its logo to the corner of its video, this is a typically visible digital watermark.

Invisible digital watermarking is a way by which anybody can hide information in digital signal and the information will not be perceived. Since it is invisible, invisible digital watermarking has a widespread use. It can be used to add identification of owner in signal and is more difficult to detect and remove. It is also possible to use embedded information to share secret or communicate in a hidden way. The invisible digital watermarking can be detected and validated by some specific technology or the people share secret with the owner. The research on digital watermarking algorithm, application and attack are most about invisible digital watermarking.

## 2.2. Common medium on watermarking

Generally, a digital watermark can be embedded into all forms of media. The most common medium are audio, video and picture. It is easy to add a visible digital watermark on a digital signal, it just needs to add some data on original signal. But to make an invisible digital is not so easy as visible digital watermarking. Different medium has different data structure, so according to different medium, various algorithms are used to add digital watermarks in signal without changing the way which original signal looks like.

## 2.3. Classification

There are various ways to classify digital watermarking, such as: by feature, by medium, by detecting process, by content, and so on. Below are some useful and effective ways:

### 2.3.1 Robustness

Robustness is one of the most important attributes of a digital watermark. A fragile digital watermark is a digital watermark that fails to be detected after the slightest modifies. A semi-fragile digital watermark is a digital watermark that resists benign transformation but fails to be detected after malignanttransformations. A robust digital watermark is a digital watermark that resists a designated class of transformations. It does not mean that a robust digital watermark is better than a fragile digital watermark. Fragile and semi-fragile digital watermarks are commonly used to detect malignant transformations and protect the integrity of the digital signal. Robust digital watermarks are often used in copy protection applications.

### 2.3.2 Capacity

It is a way to determines two different main classes of digital watermarking schemes by the length of the embedded message. In zero-bit or presence watermarking schemes, the message is conceptually zero-bit long, it is designed to detect the presence or the absence of the digital watermark in the marked object. In multiple-bit watermarking or non-zero-bit watermarking schemes, the n-bit-long stream message is modulated in the watermark.

### 2.3.3 Blindness

If a digital watermarking requires the original data for watermark, it is called non-blind watermarking. If a digital does not require the original data for watermark, it is called blind watermarking. [Chen 09] [Ameya 10]

### 2.3.4 Embedding method

If the marked signal is obtained by an additive modification, this kind embedding method is called spread-spectrum. If the marked signal is obtained by quantization, this kind embedding method is called quantization type. If the marked signal is embedded by additive modification in the spatial domain, this kind embedding method is called amplitude modulation. Spread-spectrum digital watermarks have the best robustness but weak in capacity. Quantization digital watermarks are known to be weak in robustness but have great capacity.

# 3. Algorithm in digital watermarking

Algorithm is the core of digital watermarking, a good algorithm can make the digital watermarking more robust and usable. In this section, paper will introduce spatial domain and algorithms based on it. And DWT, DHT, DCT, the three most common transform domains and some novel algorithms on it will be introduced followed.

## 3.1. Algorithms based on spatial domain.

In the early days, the digital watermarking algorithms are mainly based on spatial domain. To gray-scale images, every pixel is 8-bit, and by the Most Significant Bit begins to right Least Significant Bit, which implies the importance of data bits order. Hence, we can embed the watermarks by editing the Least Significant Bit. It is an easy and basic way in digital watermarking. But compared with the transform domain algorithms which will be traduced below, algorithms based on spatial domain are fragile.

## 3.2. DWT and some novel algorithms based on it.

The DWT (Discrete Wavelet Transform) is a powerful and useful multi-resolution decomposition method in digital watermarking. It is often applied on image processing, and has been applied to such as noise reduction, edge detection, and data compression. It is consistent with the visual perception process of human eyes. DWT can localize the signal in spatiotemporal, it is a new signal analytic theory but has already been widely used. DWT uses discrete wavelet transform to decompose the original image into four sub-bands LL1, HL1, LH1, and HH1, which can be separate into lower frequency sub-bands and higher frequency sub-bands. And the low frequency sub-band LL1 which stands for the coarse level coefficients can be further decomposed into four sub-bands LL2, HL2, LH2, and HH2. We can reach the final satisfied scale by repeat this decomposition process. The low frequency image usually has better stability against the image distortion, so most time digital watermarking based on DWT is done in the LL sub-band to be robust to various classes of attacks like filtering, collusion and compression. DWT is easy to implement and can efficiently reduce the computation time.[zhou 02] [Sun 03]

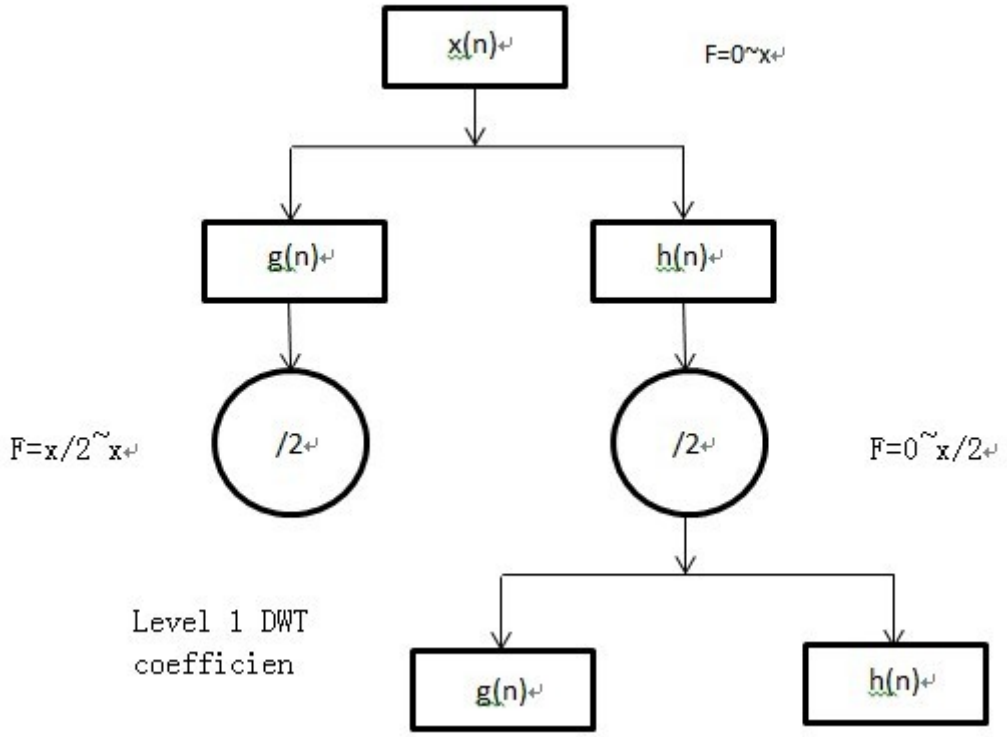


**Fig.1. Single Level DWT decomposition[Dejey 04]**

Fig.1 is process of the DWT decomposition, it is computed by successive low and high pass filtering of the discrete time domain signal. The x(n) in the Fig.1 denotes the signal. The g(n) is the low pass filter and the h(n) stands for the high pass filter. A single level of decomposition can be expressed as in Eq.1

$$Y_{\text{high}}[k] = |_n x(\text{n})(\text{g } 2\text{k} - \text{n})$$

$$Y_{\text{low}}[k] = |_n x(\text{n})(\text{h } 2\text{k} - \text{n})$$

**Eq.1 a single level of decomposition**

The decimation and filtering process is continued until we reach the desired level which depends on the length of signal. Then we concatenate all the coefficients, start from the last level of decomposition to get the DWT of the original signal.

Below are briefly introduction of some novel digital watermarking algorithms based on DWT. First is a binary image algorithm, the algorithm enhances the security of embedding watermarks by using the Logistic chaotic sequences and generalized cat mapping to scramble the watermarks. The algorithm uses an improved binary method and embeds the watermarks to the low frequency coefficients of DWT. This algorithm is robust to resist attacks like cut and salt-pepper noise. [Sun 03]. Second is an image zero-watermarking algorithm, the algorithm is used in a copyright protection zero-watermarking scheme. The algorithm decomposes the original image into the appropriate levels by the DWT, and divides the obtained approximation image into non-overlapping blocks, then use SVD (singular value decomposition)[sun 03] to get the singular values. Finally, the algorithm uses XOR operation between the first singular value of each block and pixel value of the actual binary character watermarking sequentially. This algorithm can ensure the quality of original image, and has very good robustness against the common image processing attacks.

## 3.3. DCT and some novel algorithms based on it

DCT (Discrete Cosine Transformation) is a Fourier-related transform, it only uses real numbers. DCT is roughly twice long than DFT (discrete fourier transform), operating at a finite number of real discrete data points. Like other Fourier-related transforms, DCT uses different frequencies and amplitudes to get a sum of sinusoids and then uses that sum to indicate a function or a signal. Compared with DFT or other Fourier-related transforms, DCT has different boundary conditions and only uses cosine functions. DCT is an invertible, linear function. It makes RN into RN or an N x N square matrix where R expresses the set of real numbers. The most popular form of DCT is the DCT-II which is often referred to as ¡°the DCT¡±. The formulation of DCT-II is given as Eq.2.

$$X_k = \sum_{n=1}^{N-1} \mathrm{X}_n \cos\left[\frac{\pi}{N}\left(\mathrm{n}+\frac{1}{2}\right)k\right] \qquad k = 0, \ldots\ldots, \mathrm{N}-1.$$

**Eq.2 DCT-II formulation**

In DCT-II, Xn is even around n=-1/2 and even around n=N-1/2, Xk is even around k=0 and odd around k=N, which means the boundary conditions. Below are briefly introduction of some novel digital watermarking algorithms based on DCT.

The first is a novel algorithm of audio digital watermarking based on DCT. The algorithm embeds image data into the audio signal. The algorithm decomposes the audio into some blocks. Then DCT operation is done on every block, one bit message is added by modulating AC DCT coefficient. This algorithm is robust to common attack of digital audio signal processing like low-pass filtering, adding noise and so on. [Yang 08] The second is a blind DCT domain algorithm used for biometric authentication. Use this algorithm, an entire image or logo can be embedded of hided into the original image directly. Depending on the binary bit value of watermark DCT coefficient, the algorithm change the selected DCT coefficients of the host image to odd or even values. The algorithm provides compression and authentication to biometric without using any additional data for logo extraction and introducing any specific degradation in the image quality. [Ameya 10]

## 3.4. DHT and some novel algorithms based on it

DHT (Discrete Hadamard Transformation) is a non-sinusoidal orthogonal transformation. A signal is decomposed into a set of orthogonal rectangular waveforms which are called Hadamard functions. Since the

amplitude of Hadamard functions has only two values +1 or -1, the transformation is real and has no multipliers. The Hadamard matrix is a square array of plus and minus ones whose columns and rows are orthogonal to one another. The product of an N x N Hadamard matrix and its transpose is the identity matrix. The 2D-Hadamard transform is given as Eq.3.

$$[V] = (H_n[U]H_n)/N$$

**Eq.3 2D-Hadamard transform**

Where [U] is the original image and [V] is the transformed image, H is an N x N Hadamard matrix, N=2n, n is an integer. The elements of the transform matrix Hn are binary real numbers. The inverse 2D-Hadamard transform is given as Eq.4.

$$[U] = (H_n^{-1}[UV]H_n^*) = (H_n[U]H_n)/N$$

**Eq.4 inverse 2D-Hadamard transform**

Below are briefly introduction of some novel digital watermarking algorithms based on DHT. [Franklin 05] [Ramanjaneyulu 06]

The first is an entropy based algorithm. The algorithm can use an entire image or pattern as a watermark and add it into the original image. The algorithm uses Hadamard transformation to convert cover image from spatial domain to transform domain. This algorithm is robust to random noise addition attack, cropping attack and resize attack. The second is an algorithm with MDC (Multiple Descriptions Coding) and QIM (Quantization Index Modulation). The algorithm partitions the original image into odd description and even description. DHT is applied for both two descriptions. Then the algorithm uses QIM to copy the same watermark in the first stage watermarking and embeds it. This algorithm is robust to many kinds of attacks like, JPEG, filtering, image sharpening, resizing and cropping. [Ramanjaneyulu 06]

# 4. Application of digital watermarking

Digital watermarking has been widely and successfully applied in billions of media objects across a wide range of applications. This section will introduce some applications of digital watermarking in both traditional and novel areas. Fig.2 is the basic workflow of digital watermarking. [Watermarking alliance 07]

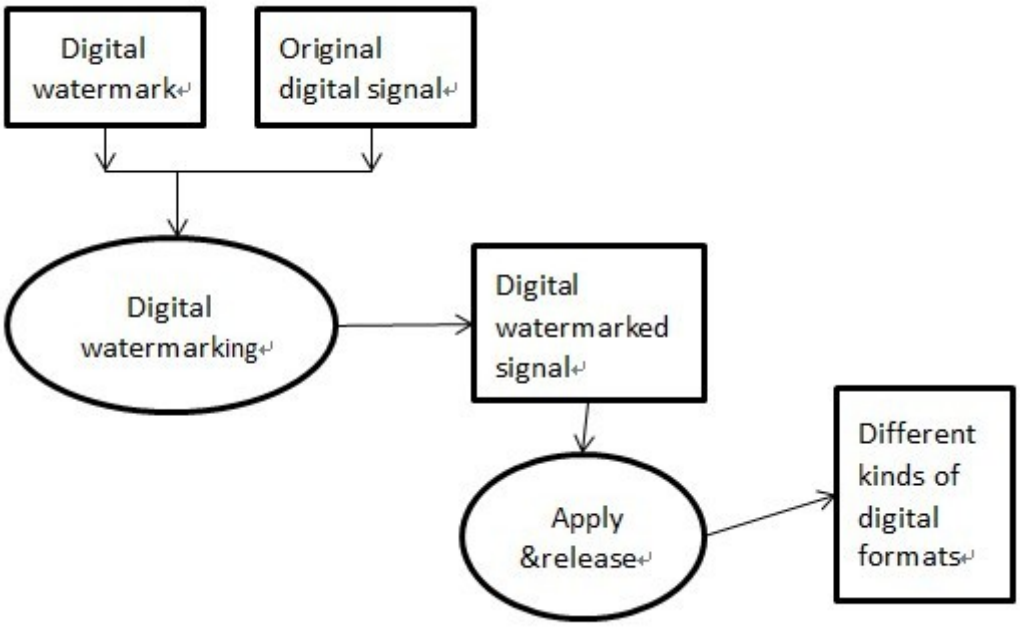


**Fig.2 workflow of digital watermarking application**

## 4.1. Application of watermarking in traditional area.

### 4.1.1 Ownership and copyrights

It is essential to communicate our copyright ownership and usage rights no matter we are global media corporations or freelance photographers. Digital content is travelling faster and further than ever before since the combination of access and new tools. Digital has become a primary means of expression and communication. We can embed watermarks which contain imperceptible digital data that can include ownership information, contact details, usage rights and anything we choose. For people who are looking for an efficient way to monitor, manage and monetize their digital assets, digital watermarking is an effective way and is widely used today. Digital watermarking can ensure our ownership and contact information are attached to our content, and can add automated licensing to increase revenues, automated remind us when there is an unauthorized use.

### 4.1.2 Document and image security

Nowadays is a corporate world, documents and images travel more rapidly and widely through Internet. We can only know a little about who is accessing our documents and images and where our documents and images are being accessed. We can use digital watermarking to embed a unique digital ID into documents and images, which can easily be detected by devices but undetectable to humans. For example, a unique digital watermark can be embedded into each copy of a document once they are being created or distributed. Using digital watermarking, it is easy to trace back to the source when any information is leaked. Besides, companies can use software to add or detect digital watermarks, and even can use the devices with watermark detector. For instance, we can prevent someone from attempting to copy our security documents with watermarks by using a printer with watermark detector.

### 4.1.3 Protection for audio and video content

In global entertainment industry, piracy of music, film and video is a multi-billion dollar big problem. Digital watermarking can help limit the unauthorized copy and redistribute, it can provide an added layer of security to the content protection. Digital watermarking can communicate copyright ownership and rights of usage, protect content against common threats of piracy like camcorder recording, Peer to Peer sharing, copying, format conversion and other forms of re-processing. We can enjoy our entertainment experience without any difference even if the content has embedded watermarks.

## 4.2. Application of watermarking in novel area

### 4.2.1 Locating content online

Since we rely more and more on the Internet for information sharing, customer engagement, research and communication, we have to upload more and more content to the web. For instance, if you are a photographer or artist, you have a vast content you¡¯d like to share on the web. The problem is you will risk losing control of your valuable assets once you post your content online. And if you are a network seller, you want showcase your products and engage more buyer, but you don¡¯t who will use the information of you and your products. Using digital watermarking can help we get fair compensation for our content usage, make sure that the right content is used on the right sites at the right time, gather information by where and what are accessed, give us a warning when unauthorized usage is detected.

### 4.2.2 Rich media enhancement for mobile phones

To most of us, mobile phones are no longer merely for talking or texting. We use mobile phones more and more to find assistance, information and entertainment. Thousands of media companies want to popularize their products like newspapers and magazines. Since watermark can be embedded into all forms of media easily, it is a good way for companies to engage consumers by enriching their media experiences on their mobile phones with protected media content. Digital watermarking can help companies engage and retain more consumers, create brand preference and loyalty, bring traditional printed like newspaper and magazines to the Internet.

# 5. Attack on digital watermarking

Attack on digital watermarking is another important area in digital watermarking. By studying different attacks, we can find drawbacks on algorithms and schemes, and find ways against the attacks, improve the security of digital watermarking. In this section, some common attacks and some novel attacks will be introduced.

## 5.1. Common attacks on digital watermarking

Copy attack is one of the most common attacks on digital watermarking. We can consider the watermark as noise in the original digital signal, the attacker can somehow estimate the original digital signal. Actually, there are various researches are about how to filter the additive noise from digital signal, this means the attackers can use these recent advanced research result to estimate or remove the watermarks. We use a digital watermark to protect a piece of media such as an image, film or audio. If a piece of media is found to lack a watermark, it would be regarded as unauthenticated. In copy attack, the attackers estimate the watermark on an original media, and then add that watermark into an unauthenticated new piece so that the watermark can not protect the copyright of the media. [Wikipedia 14] Removal attack is another common attack on digital watermarking. Removal attack is acting by removing the watermark from the original signal. It includes a lot of methods, like denoising, lossy compression, quantization, demodulation, averaging attacks

and collusion. [Ehsan 01]

### 5.2. Some new attack technology on digital watermarking

Since the digital watermarking algorithms are becoming more and more robust, more and more new attacks on digital watermarking are emerging. Below is a brief introduction about some new attacks.

The first is a new adaptive watermarking attack in wavelet domain. This attack will find the flat regions, edges and textures of an image which has been embedded with watermarks. Then the attack will manipulate the wavelet coefficients of each region separately so that the watermarks will be destroyed and the original image will has the least visual distortion. This attack has been proved that is effective on some robust watermarking methods. The average Peak Signal to Noise Ratio is more than 31dB after applying the proposed attack. [Taherinia 12]

The second is a self-similarities attack. The attack tries to substitute some parts of the image with some other parts of itself which are similar. By this, the watermark will be destroyed and the original signal will keep clear. In the basic version of this attack, the original image is being separated into blocks, and one block is associated with another block which is similar according to a Root Mean Square metric. In the improved version of this attack, several blocks are combined to computer the replacement of one block. Principal Component Analysis is used on blocks to build the efficient codebook. This attack can break the watermarks, but sometimes is difficult to keep the Peak Signal to Noise Ratio in a good level. [Bennour 13]

## 6.Summary

This survey paper starts from some basic knowledge of digital watermarking, includes the classification and medium of digital watermarking. There are various kinds of digital watermarking on different medium with different attribution.

Then paper gives a brief introduction about digital watermarking algorithm. Algorithm based on spatial domain is important in early days, it is easy to compute but it is also fragile. Most algorithms now are based on transform domain, DWT, DHT, DCT are three commonly used transform domain. Most of the novel algorithms based on transform domain are easy to compute and achieve, at the same time, are robust to common attacks.

Digital watermarking has a widely application, including copyright protection, content protection, locating content online, and so on. Some traditional application and some novel application are introduced in the paper. In conclusion, digital watermarking gives authentication, identification, and integrity to digital signal, and helps the owners can use their digital assets under protection.

Accompany with the development of digital watermarking, more and more attacks on digital watermarking are emerging. Some common attacks and novel attacks are shown in the paper. All of them are threating the security of digital contents. But in the other hand, attacks promote the development of digital watermarking. With the rapid development of digital technology, people use digital signal to communicate, share information and save data more frequently, digital watermarking can provide security protection for both individuals and companies, and will keep developing rapid and play an important role in the future network.

## 7.References

[Ehsan 01]Ehsan Syed; "Final Report of Digital Watermarking"; University of Texas at Arlington; 2011; http://www-ee.uta.edu/Dip/Courses/EE5359/2011SpringFinalReportPPT

/Syed_EE5359Spring2011FinalPPT.pdf

[Zhou 02]Yaxun Zhou, Wei Jin; "A novel image zero-watermarking scheme based on DWT-SVD"; Multimedia Technology (ICMT), 2011 International Conference; Date: Aug, 2011; Pages:2873-2876; http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6002066

[Sun 03]TianKai Sun, XiaoGen Shao, XingYuan Wang; "A Novel Binary Image Digital Watermarking Algorithm Based on DWT and Chaotic Encryption"; Young Computer Scientists, 2008. ICYCS 2008; Date: Dec, 2008; Pages: 2797-2802; http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4709424

[Dejey 04] Dejey, R.S. Rajesh; "Robust Color Image Watermarking Schemes In the Wavelet Domain"; ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING, issue 01; Date: Aug, 2010; http://dc219.4shared.com/doc/2k9VCgnH/preview.html

[Franklin 05] Franklin Rajkumar.V, Manekandan.GRS, V.Santhi; "Entropy based Robust Watermarking Scheme using Hadamard Transformation Technique"; International Journal of Computer Applications; Number 9 - Article 4; Date:2011; http://www.ijcaonline.org/volume12/number9/pxc3872293.pdf

[Ramanjaneyulu 06] K. Ramanjaneyulu1, K. Rajarajeswari; "An Oblivious and Robust Multiple Image Watermarking Scheme Using Genetic Algorithm"; The International journal of Multimedia & Its Applications (IJMA) Vol.2, No.3; Date: Aug, 2010; http://airccse.org/journal/jma/0810ijma02.pdf

[Watermarking alliance 07]Digital watermarking alliance, 2011; http://www.digitalwatermarkingalliance.org/applications.asp

[Yang 08]Yan Yang, Rong Huang, Mintao Xu; "A Novel Audio Watermarking Algorithm for Copyright Protection Based on DCT"; Electronic Commerce and Security, Second International Symposium; Date: Oct 2009; Pages: 184-188; http://ieeexplore.ieee.org.libproxy.wustl.edu/stamp/stamp.jsp?tp=&arnumber=5210002

[Chen 09] Liwei Chen, Mingfu Li; "An Effective Blind Watermark Algorithm Based on DCT*"; Intelligent Control and Automation, 2008; Date: Aug, 2008; Pages: 6822-6825; http://ieeexplore.ieee.org.libproxy.wustl.edu/stamp/stamp.jsp?tp=&arnumber=4593967

[Ameya 10] Ameya K. Naik, Raghunath S. Holambe; "A Blind DCT Domain Digital Watermarking for Biometric Authentication"; Intelligent Control and Automation; International Journal of Computer Applications; Number 16 - Article 3; Date: 2010; http://www.ijcaonline.org/journal/number16/pxc387529.pdf

[Kim 11] Jungyeop Kim, Sungmin Won, Wenjun Zeng, Soohong Park; "Copyright protection of vector map using digital watermarking in the spatial domain"; Digital Content, Multimedia Technology and its Applications (IDCTA), 2011 7th International Conference; Date: Dec, 2011; Pages: 154-159; http://ieeexplore.ieee.org.libproxy.wustl.edu/stamp/stamp.jsp?tp=&arnumber=6016651

[Taherinia 12] Taherinia, A.H, Jamzad, M.; "A new adaptive watermarking attack in wavelet domain"; Multimedia, Signal Processing and Communication Technologies; Date: Jul, 2009; Pages: 320-323; http://ieeexplore.ieee.org.libproxy.wustl.edu/stamp/stamp.jsp?tp=&arnumber=5164240

[Bennour 13] Bennour, Jihane;Dugelay, Jean-Luc, Matta, Federico; "Watermarking Attack (BOWS contest)"; Security, Steganography, and Watermarking of Multimedia Contents IX part of Electronic Imaging,

Date: Feb, 2007;
http://www.eurecom.fr/util/publidownload.fr.htm?id=2109

[Wikipedia 14] Copy attack, 2011;
http://en.wikipedia.org/wiki/Copy_attack

[Wikipedia 15] Digital watermarking, 2011;
http://en.wikipedia.org/wiki/Digital_watermarking

# 8.List of Acronyms

| | |
|---|---|
| DCT | Discrete Cosine Transformation |
| DHT | Discrete Hadamard Transformation |
| DWT | Discrete Wavelet Transform |

---

Last modified: Nov 27, 2011
This and other papers on latest advances in network security are available on line at
http://www1.cse.wustl.edu/~jain/cse571-11/index.html
Back to Raj Jain's Home Page