

# A Communication System Model for Digital Image Watermarking Problems

Pei-chun Chen  
Department of Electrical Engineering  
National Tsing Hua University  
Hsinchu 300, Taiwan, R.O.C.

And

Yung-sheng Chen  
Department of Electrical Engineering  
Yuan-Ze University  
Chung-Li 320, Taiwan, R.O.C.

And

Wen-hsing Hsu  
Department of Electrical Engineering  
National Tsing Hua University  
Hsinchu 300, Taiwan, R.O.C.

## ABSTRACT

As the Internet becomes more and more populous, people concern more about the copyright protection issue for digital data such as images and audio. Digital watermarking technique can hide data in images or audio to indicate the data owner or recipient. Therefore, it can protect the copyright. There were a lot of papers discussing how to embed watermark into images in recent years. However, few papers analyzed the watermark techniques in a theoretical point of view. In this paper, we interpret the watermarking problem as a digital communication problem. There are three main criteria concerning the performance of a watermarking technique- capacity, imperceptibility, and robustness. We then show the trade-off's between these three criteria adopting concepts from the digital communication theory.

## 1 INTRODUCTION

With the prevalence of the Internet, more and more digital data can be accessed via the network. Internet users can transmit and store images, videos, and audio without offering appropriate credits to the creator. This hinders creator from sharing his works in the Internet. Digital watermarking technique is a solution to the copyright protection problem of digital media. In addition to *copyright protection*, digital watermark has various other applications, such as:

- *Recipient marker* Recipient information can be embedded in the original image to trace the image distribution.
- *Image fingerprinting (authentication)* Image fingerprint (watermark) acts as a checksum or hash result of an image to signal any alteration of the original image.
- *Hidden annotation* Hidden annotation (watermark) can carries patient information in a medical image. It can also help in a content-based retrieval, or serves as a multimedia index.
- *Secret communication* Secret information is hidden in an image imperceptibly. In this application, a secret key is required to retrieve hidden information in the image.

In 1994, van Schyndel et al. [6] changed the LSB of an image to embed a m-sequence watermark. Since then, more and more researchers studied digital watermarking problem. Digital watermarking technique evolved from how to embed a watermark in an image to how to improve the robustness of the watermark. However, there lacks complete mathematical analyzes on performance of watermarking techniques. The test results applied to some specific images were not convincing enough either. In this paper, a noble analyze of digital image watermarking problem using concepts from digital communications is presented.

In general, watermark can be embedded in *spatial domain* or *transform domain* of an image. In the spatial domain approach, such as [6, 2], the pixel value of an image is modified to embed watermark information; In the transform domain approach, such as [3], some transform is applied to the original image first. The transform applied may be DFT, DCT, or DWT, etc. The watermark is embedded by modifying the transform domain coefficients. Empirically, The transform domain approaches are more robust against noise or attack.

As mention in the first paragraph , digital watermarking has many applications. Different applications has different requirements. There are no general requirements for all watermarking problems. In this paper, we concern about copyright protection application of image data. The concepts discussed can apply to other media such as video as well. According to [5], requirements of copyright protection watermark include but are not constrained to:

1. *Public watermark* The watermark retrieval process should be *public*, in which no original image is needed, to reduce data transmission number and improve the security. On the other hand, the *private* watermarking scheme needs the original image in the watermark retrieval process.
2. *Imperceptibility (Perceptual transparency) of an Invisible Watermark* Invisible watermark should be imperceptible to avoid interrupting the viewing experience.
3. *Maximal capacity* We would like more information carried by a digital watermark in an original image.
4. *Robustness against image manipulations*
  - additive Gaussian or non-Gaussian noise;
  - filtering, both linear and nonlinear filtering;
  - compression, e.g. JPEG;
  - local exchange of samples;
  - affine transform of image, e.g., rotation and rescaling of image;
  - averaging multiple watermarked copies of an image;
  - D/A and A/D conversions, e.g. printing and scanning of an image;

The later three criteria, *imperceptibility*, *maximal capacity*, and *robustness*, can not be achieved at the same time. The reason for the conflict is revealed by the formula derived in Section 2.

In the next section, the reader is first oriented with some background and definitions of the watermarking problem. Two ways of analyzing the criteria conflict in

a watermarking problem are then presented. In Section 3, we discuss from the *channel capacity* point of view. *Probability of error* of a detected watermark under some level of noise resulted from image manipulations is calculated in Section 4.

## 2 Communication System Realization of Digital Image Watermarking Problem

In a digital image watermarking system, information carrying watermark is embedded in an original image. The watermarked image is then transmitted or stored. The received corrupted watermarked image is then decoded to resolve the watermark. The brief watermarking system flowchart is sketched in Figure 1. With notification similar to describing a communication system, the detailed flowchart of a watermarking system is presented in Figure 2.

This watermark insertion and detection model view the watermarking problem as a spread spectrum digital communication problem. Watermark is the message, while the original image is the channel. In the watermark detection stage, the original image acts as a noise to the watermark message. Therefore, we can adopt concepts from the digital communication system to analyze the digital image watermarking problem.

## 3 Channel Capacity of the original image

We begin this section with some definitions.

**Definition 3.0.1** 1. Consider the original image as a discrete-time random process.

$$\tilde{X} = (X_1 \ X_2 \ \cdots \ X_N)^T \quad (1)$$

2. Consider the watermark as a discrete-time random process too.  $W_i$ ,  $1 \leq i \leq N$ . Therefore, a watermarked image is:

$$Y_i = X_i + W_i, \quad 1 \leq i \leq N \quad (2)$$

3. A watermarked image after some image manipulations:

$$R_i = f(X_i + W_i) = X_i + W_i + T_i, \quad 1 \leq i \leq N \quad (3)$$

The last equal sign is a linear approximation to function  $f(\cdot)$ .

◇

The sufficient statistics for detection is  $\langle R_i, W_i \rangle$ .

$$\langle R_i, W_i \rangle = \langle X_i, W_i \rangle + \langle W_i, W_i \rangle + \langle T_i, W_i \rangle \quad (4)$$

According to the equation above, a private watermark detection scheme without projection of the original image,  $\langle X_i, W_i \rangle$ , has smaller noise value. Therefore, its probability of error is smaller.

As mentioned earlier in Section 1, the three digital image watermarking criteria, *maximal capacity*, *robustness*, and *imperceptibility*, are trade-off's. In this subsection, we define these three terms as in the following. Note that in Section 4, we will define these three terms in a different way.

**Definition 3.0.2 (Maximal Capacity)** *The Maximal Capacity is bounded by the "channel capacity" of the original image.*

◇

**Definition 3.0.3 (Robustness)** *According to Shannon's Channel Coding Theorem [1], reliable communication is achieved if the transmission rate is lower than the channel capacity.*

$$R < C \Rightarrow \text{reliable communication}$$

Therefore, successful watermark detection is guaranteed if the total bits embedded in an original image is smaller than the channel capacity calculated.

◇

**Definition 3.0.4 (Imperceptibility)** *Imperceptibility is achieved by*

1. *Low SNR (Signal to Noise Ratio)  $\frac{\gamma^2}{\sigma^2}$ , where "signal" refers to the watermark and "noise" refers to the original image. See (5) and (9) for the definition of  $\sigma^2$  and  $\gamma^2$ .*
2. *High Correlation between the watermark and the original image  $\frac{\text{Cov}(W_i, X_i)}{\sqrt{\text{Var}(W_i) \text{Var}(X_i)}}$ .*

◇

### 3.1 Memoryless channel and source model

First we consider the original image and watermark as memoryless channel and source. This could be done after properly source coding of the original image. Take Karhunen-Loève transform for example. It can turn the image into N independent channels, or say, dimensions. This number, N, is image dependent.

The channel capacity  $C \stackrel{\text{def}}{=} \max_{p(\tilde{W})} I(\tilde{W}; \tilde{R})$  is then calculated. Assume this is a Gaussian channel. Gaussian channel has the lowest channel capacity among all.

$$X_i \sim N(0, \sigma_i^2), \quad 1 \leq i \leq N \quad (5)$$

The watermark power is constrained by the human visual perceptibility to have a total power of S.

$$\sum_{i=1}^N E[W_i^2] \leq S \quad (6)$$

Then,

$$C(S) = \sum_{i=1}^N \frac{1}{2} \log_2 \left( 1 + \frac{\gamma_i^2}{\sigma_i^2} \right) \quad (7)$$

where

$$\gamma_i^2 = \max[0, \theta - \sigma_i^2] \quad (8)$$

$$\sum_{i=1}^N \gamma_i^2 = S \quad (9)$$

If we take  $T_i$  into account,  $T_i$  along with  $X_i$  are noises to  $W_i$ . The corresponding noise power  $\sigma_i^2$  is replaced by  $\sigma_i'^2$ .

$$\text{Noise} = X_i + T_i \quad (10)$$

$$\sigma_i'^2 = \sigma_i^2 + \sigma_{T_i}^2 + 2\text{Cov}(X_i, T_i) \quad (11)$$

$$C(S) \simeq \sum_{i=1}^N \frac{1}{2} \log_2 \left( 1 + \frac{\gamma_i^2}{\sigma_i^2 + \sigma_{T_i}^2 + 2\text{Cov}(X_i, T_i)} \right) \quad (12)$$

Compare (12) with (7), with manipulation considered, the channel capacity decreases. In addition to the original noise power  $\sigma_i^2$ , noise power introduced by manipulations  $\sigma_{T_i}^2$  and covariance between  $X_i$  and  $T_i$  contributes to the total noise power  $\sigma_i'^2$ .

$$\sigma_i'^2 \stackrel{\text{usually}}{<} \sigma_i^2 + \sigma_{T_i}^2 + 2\sigma_i^2 \quad (13)$$

$$= 3\sigma_i^2 + \sigma_{T_i}^2 \quad (14)$$

$$\simeq 3\sigma_i^2 \quad (15)$$

$$C(S) \simeq \sum_{i=1}^N \frac{1}{2} \log_2 \left( 1 + \frac{\gamma_i^2}{3\sigma_i^2} \right) \quad (16)$$

If  $\sigma_i^2 = \sigma^2$  for all  $i$ , we can simplify (7), (8), and (9)

$$C(S) = \frac{N}{2} \log_2 \left( 1 + \frac{\gamma^2}{\sigma^2} \right) \quad (17)$$

$$\gamma^2 = \frac{S}{N} \quad (18)$$

Since  $\gamma^2 \ll \sigma^2$ , we further simplify the equation,

$$C(S) \simeq \frac{N}{2} (\log_2 e) \left( \frac{\gamma^2}{\sigma^2} \right) \quad (19)$$

Take  $T_i$  into account and apply result obtained in (15).

$$C(S) \simeq \frac{N}{2} (\log_2 e) \left( \frac{\gamma^2}{3\sigma^2} \right) \quad (20)$$

Some important results derived from the above derivations are worth discussing. First, from (7), (12), (16), (17) and (20), the larger the watermark power, the greater the capacity value. While greater watermark power implies weaker imperceptibility (Definition 3.0.4), this means capacity and imperceptibility conflict. The later two equations (17) and (20), although a simplified version, clearly show us the trade-off between imperceptibility and capacity.

Second, as mention in Definition 3.0.4, the second criteria judging if a watermark inserted is imperceptible is the correlation between the watermark and the original. Therefore, the watermark is designed to maximize the the correlation. In (5), we assume the original image as a Gaussian channel. The correlation is maximized if the watermark signal is also Gaussian. This explains why [3] choose Gaussian signal as a watermark.

### 3.2 Markov channel and source model

Consider a Markov-n channel. Let  $Q(\tilde{y}|\tilde{x}) = Q(y_1, \dots, y_n|x_1, \dots, x_n)$  be the probability of block output  $(y_1, \dots, y_n)$ , given block input  $(x_1, \dots, x_n)$ , of a discrete-time stationary channel. Then the capacity of this channel is

$$C(S) = \lim_{n \rightarrow \infty} \frac{1}{n} C_n(nS) \quad (21)$$

where

$$C_n(S(\theta)) = n^{-1} \sum_{i=1}^n \max[0, \frac{1}{2} \log_2(1 + \frac{\gamma_i^2}{\sigma_i^2})] \quad (22)$$

$$= n^{-1} \sum_{i=1}^n \max[0, \frac{1}{2} \log_2(1 + \frac{\theta}{\sigma_i^2})] \quad (23)$$

$$S(\theta) = \sum_{i=1}^n \max[0, \theta - \sigma_i^2] \quad (24)$$

Take the limit, (21) gives

$$C(S_\theta) = \frac{1}{2} \int_{-\frac{1}{2}}^{\frac{1}{2}} \max[0, \log_2 \frac{\theta}{N(f)}] df \quad (25)$$

$$S_\theta = \int_{-\frac{1}{2}}^{\frac{1}{2}} \max[0, \theta - N(f)] df \quad (26)$$

where  $N(f)$  is the noise power spectral density.

$$N(f) = \sum_{k=-\infty}^{\infty} \phi_k \exp^{-j2\pi kf} \quad (27)$$

and  $\phi_k$  is the noise autocorrelation function. Refer to [1] for details.

The relation between capacity and watermark power is not explicitly shown in (25) as in Section 3.1. The relation is still the same, the larger the watermark power,

the greater the capacity value. Since the channel and source is not memoryless, noise in one index  $k$  will propagate to others. Thus, instead of using single term  $\sigma_i^2$  and summing all  $i$ 's,  $N(f)$  is used and integral is taken.

## 4 Error Rate of the Watermark Detector

In this section, we define *capacity*, *robustness*, and *imperceptibility* in a different way.

**Definition 4.0.1 (Capacity)** After source coding in Figure 2, if the watermark codeword set has  $M = 2^k$  codewords, then its capacity is  $M$ .

◇

**Definition 4.0.2 (Robustness)** Error rate performance  $P_e$  is defined to be the measure of robustness.

◇

**Definition 4.0.3 (Imperceptibility)** Similar to Definition 3.0.4, imperceptibility is achieved by larger value of the “jamming margin”,  $\frac{J_{av}}{P_{av}}$ , where  $J_{av}$  refers to the average power of the original image and  $P_{av}$  refers to the average power of the watermark signal.

◇

From [4], the probability of error of a detector of a communication system in Figure 2 is union bounded as

$$P_e \leq \sum_{m=2}^M Q \left( \sqrt{\frac{(\frac{2W}{R})}{(\frac{J_{av}}{P_{av}})} R_c W_m} \right) \quad (28)$$

$$\leq (M-1)Q \left( \sqrt{\frac{(\frac{2W}{R})}{(\frac{J_{av}}{P_{av}})} R_c W_m} \right) \quad (29)$$

where  $\frac{W}{R}$  is the “processing gain” resulting from spread spectrum communication.

$$\frac{W}{R} = \frac{T_b}{T_c} = \frac{\text{data interval}}{\text{chip interval}} \quad (30)$$

and  $R_c W_m$  is the “coding gain” resulting from error correction coding.

$$R_c = \frac{k}{n} \quad (31)$$

$$W_m = \min_{\text{Codeword Set}} \text{weight} \quad (32)$$

Note that  $Q(\cdot)$  is monotone decreasing function.

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} \exp^{-\frac{t^2}{2}} dt, \quad x \geq 0 \quad (33)$$

From (28) and (29) above, the relations between probability of error, capacity, processing gain, jamming margin, and coding gain are clear. With other control variables fixed,

- Capacity  $\uparrow \Rightarrow$  Probability of error  $\uparrow$ . More errors occurs as more bits are embedded in an image.
- Processing gain  $\uparrow \Rightarrow$  Probability of error  $\downarrow$ . The broader the spread spectrum codes spread, the smaller the error rate.
- Jamming margin  $\uparrow \Rightarrow$  Probability of error  $\uparrow$ . Increasing the watermark power reduces the error rate. In this case, watermark is more visible.
- Coding gain  $\uparrow \Rightarrow$  Probability of error  $\downarrow$ . The introduction of error correction codes reduces the probability of error.

## References

- [1] Richard E. Blahut. *Principle and Practice of Information Theory*, chapter 7. Addison-Wesley, 1987.
- [2] Gordon W. Braudaway. Protecting publicly-available images with an invisible image watermark. In *Proceedings, 1997 IEEE International Conference on Image Processing*, pages 524–527, Santa Barbara, CA, U.S.A., Oct. 1997.
- [3] Ingemar J. Cox, Joe Kilian, Tom Leighton, and Talal Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Trans. on Image Processing*, 6(12):1673–1687, June 1997.
- [4] John G. Proakis. *Digital Communications*, chapter 5, 13. McGraw-Hill, 3rd edition, 1995.
- [5] Mitchell D. Swanson, Mei Kobayashi, and Ahmed H. Tewfik. Multimedia data-embedding and watermarking technologies. *Proceedings of the IEEE*, 86(6):1064–1087, June 1998.
- [6] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. A digital watermark. In *Proceedings, 1994 IEEE 1st International Conference on Image Processing*, pages 86–90, Singapore, Nov. 1994.

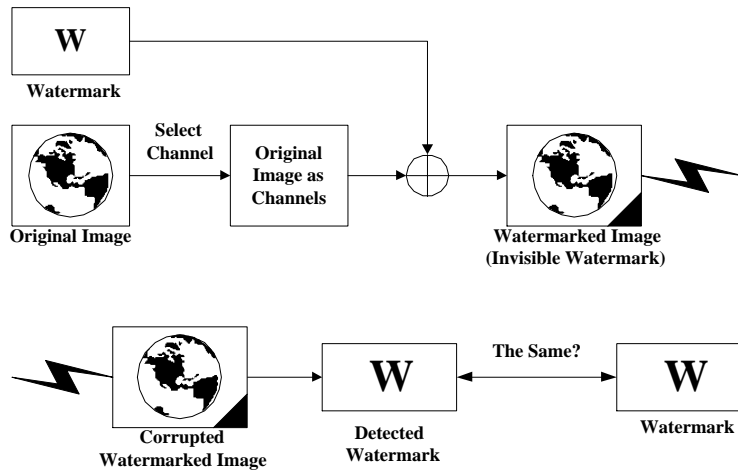


Figure 1: A General Watermarking System.

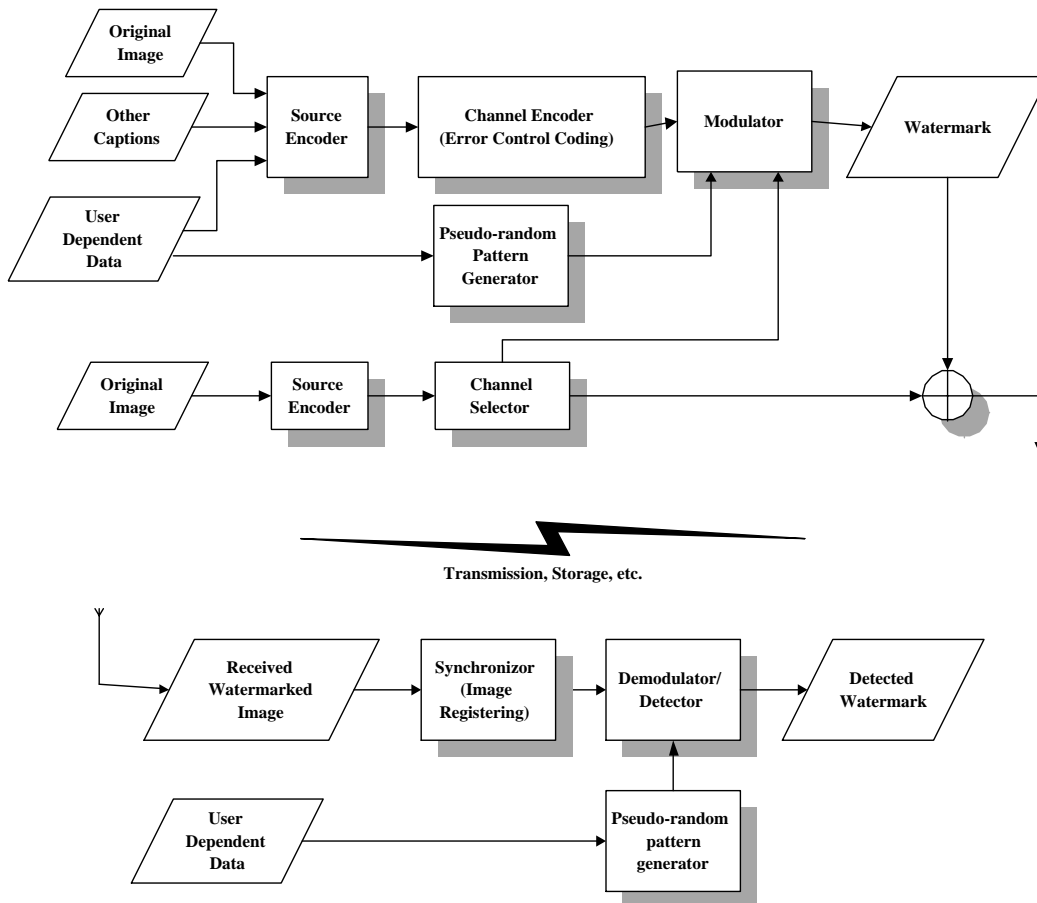


Figure 2: The Watermark Insertion and Detection Model.

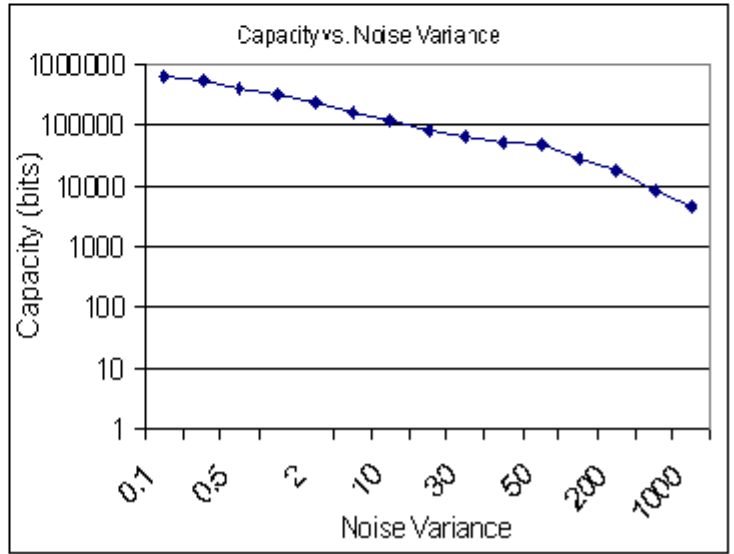
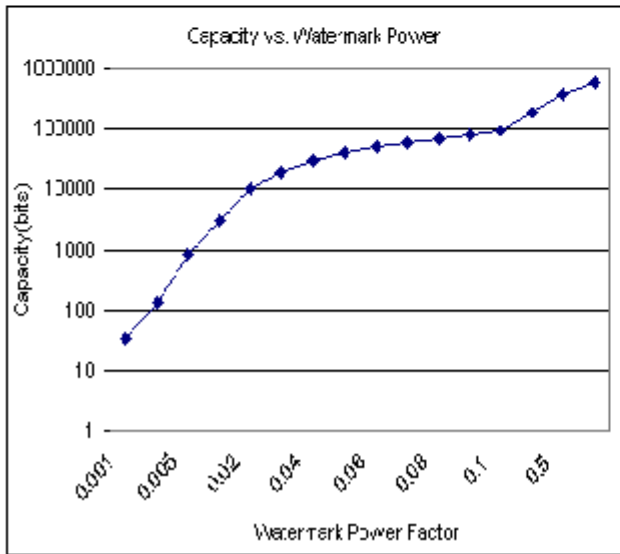


Figure 3: Experiment.