

# Practical Capacity of Digital Watermarks

Ryo SUGIHARA  
IBM Tokyo Research Laboratory  
sugiryo@jp.ibm.com

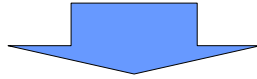
# "WM" : watermark

## Background

- Capacity issue on digital WMs
  - "Channel capacity of WM channel"
  - "How to model the WM channel?"
- However, there are problems.
  - Hard to achieve : assuming an ideal code
  - Lack of discussion for "Reliability"
    - Error-free attribute is asymptotically realized

## Aim of this study

- Necessity for “practical” capacity
  - On design : need to determine the payload
  - On operation : need to assure reliability of WM system



- We want to know.....  
“How many bits can be embedded with satisfying the conditions on reliability?”



**“Practical” Capacity**

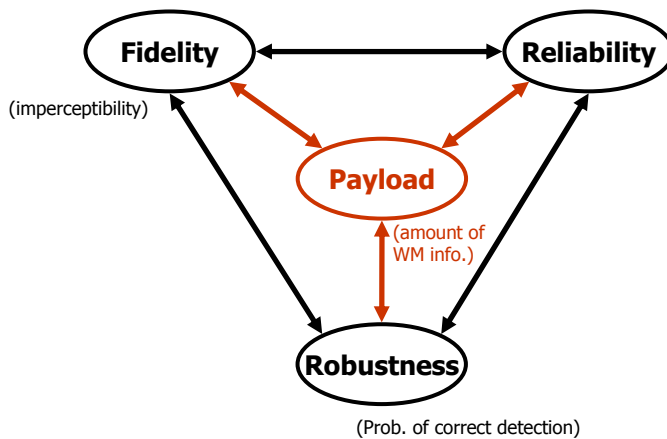
## Our approach

- Modeling the WM scheme
  - Assumptions on its statistical characteristics
- Formulate the reliability
- Determine the threshold for detection
  - Satisfying the predetermined requirements on reliability
- Determine the practical capacity

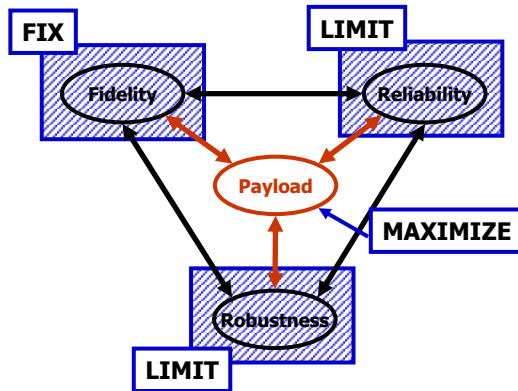
## Overview

- Background & aim of this study
- **Problem definition**
- Theoretical analysis on capacity
- Experiments
- Conclusion & future works

## Trade-offs in WMing



## Problem definition

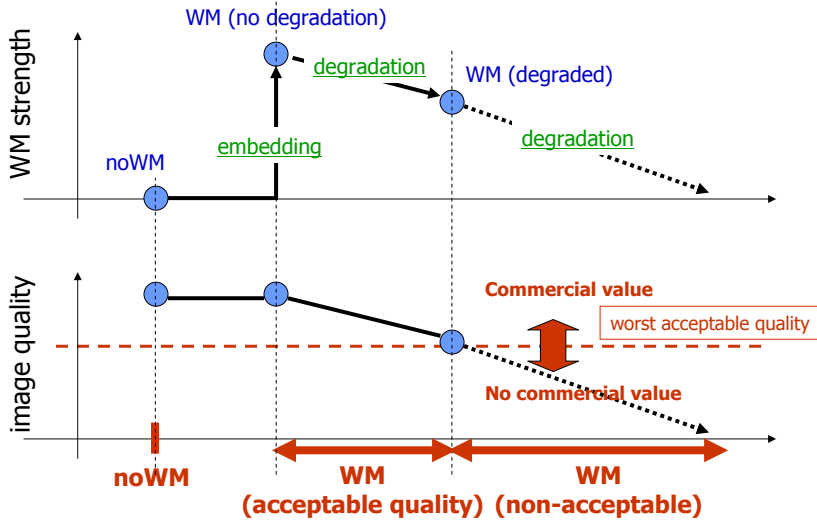


"Practical" capacity  $\equiv$  Maximum payload  
which satisfies the limitations

## Measurements of reliability & robustness

	Probability
<u>No watermark embedded (noWM)</u>	
not detected	$1 - P_f$
detected (false alarm)	$P_f$
-----	
<u>Watermark embedded (WM)</u>	
not detected	$1 - (P_c + P_e)$
detected	<ul style="list-style-type: none"> <li>correct extraction <math>P_c</math></li> <li>erroneous extraction <math>P_e</math></li> </ul>

## Problem definition : stages of WM



## Problem definition : limitations

	noWM (case: 1)	WM	
		acceptable quality (case: 2a)	non- acceptable (case: 2b)
$P_f$ (false alarm)	$< P_{fmax}$		
$P_c$ (correct extraction)		$> P_{cmin}$	—
$P_e$ (erroneous extraction)		$< P_{emax}$	

- In case 1, prob. of false alarm is upper-bounded
- In case 2a, prob. of correct extraction is lower-bounded

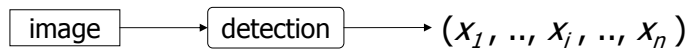
**"Practical" capacity = maximum amount of payload**

- since it should not occur even if image is degraded (e.g. copy-control purpose)

## Overview

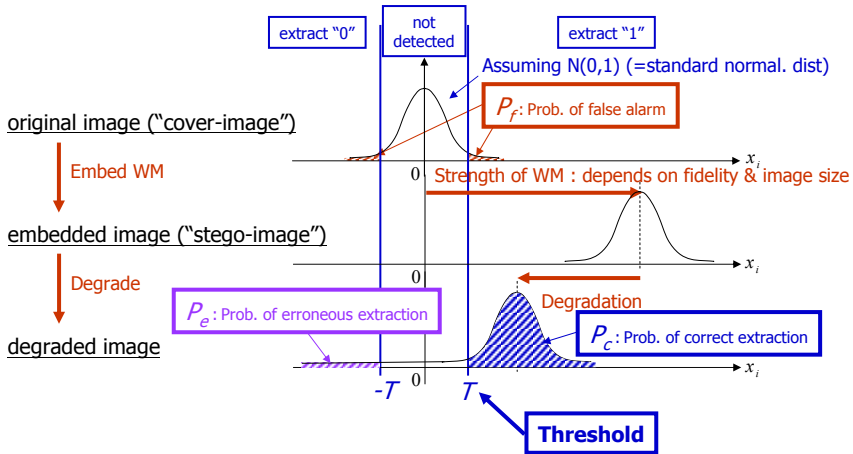
- Background & aim of this study
- Problem definition
- Theoretical analysis on capacity
  - Assumptions on WM scheme
  - Formulation of reliability & robustness
- Experiments
- Conclusion & future works

## Assumptions on WMing scheme



- In case of embedding  $n$ -bit message.....
  - A detection yields an  $n$ -dimensional vector  $\{x_j\}$
  - $|x_j|$  stands for the strength of WM
  - Each  $x_j$  is i.i.d. (independent and identically distributed)

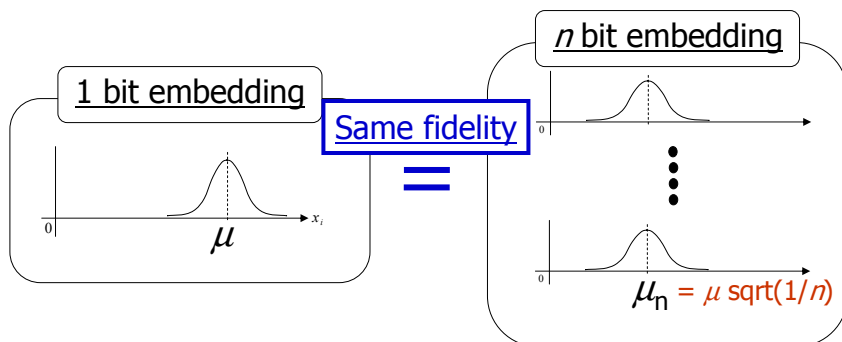
## In case of embedding 1 bit...



**Threshold controls each of the probability**

## In case of $n$ bits.....

- The center of distribution changes with  $n$ 
  - in proportion to  $\sqrt{1/n}$



$$(WM \text{ strength}) = \mu_n \sqrt{n} (= \mu)$$

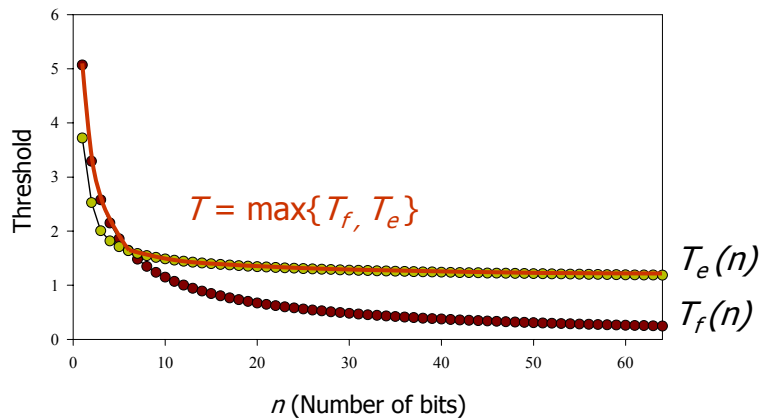
## In case of $n$ bits..... (continued)

- Detection criteria:
  - “Detect WM” if  $|x_i|$  exceeds the threshold for all  $i$ 's
- $P_f, P_e$  and  $P_c$  can be formulated
  - as functions of  $n$  (number of bits)
- Threshold values for
  - satisfying  $P_f < P_{fmax}$   $\longrightarrow T_f(n)$
  - satisfying  $P_e < P_{emax}$   $\longrightarrow T_e(n)$

function of  $n$

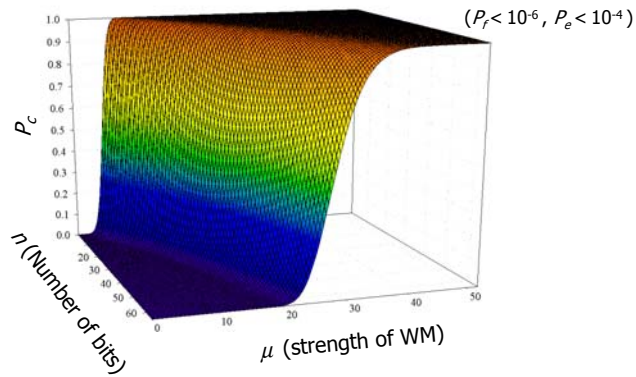
## Threshold values

- Example :  $P_f < 10^{-6}$  ,  $P_e < 10^{-4}$



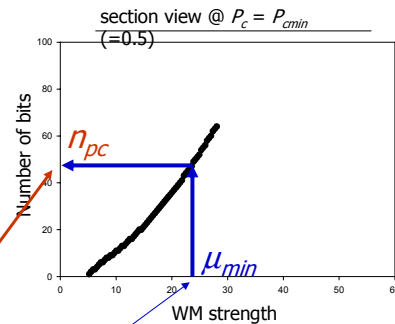
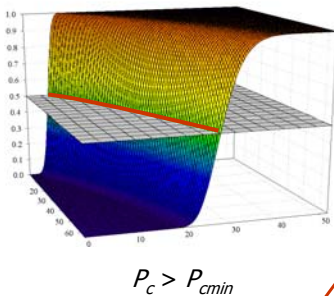
## Theoretical prob. of correct extraction

- $P_c$  can be derived as a function of  $n$  (number of bits) and  $\mu$  (strength of WM)



## Theoretical capacity analysis

Example



**Practical capacity**

## Overview

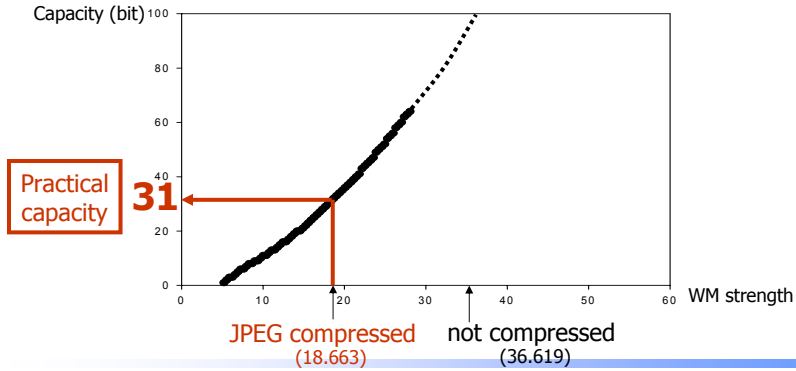
- Background & aim of this study
- Problem definition
- Theoretical analysis on capacity
- Experiments
- Conclusion & future works

## Experimental conditions

- Limitations:  $P_f < 10^{-6}$ ,  $P_e < 10^{-4}$ ,  $P_c > 0.5$
- Worst acceptable quality: JPEG (Quality : 80)
  
- Patchwork-based method
  - Modified for multiple bit embedding
- Tested on 1000 images (640x426)

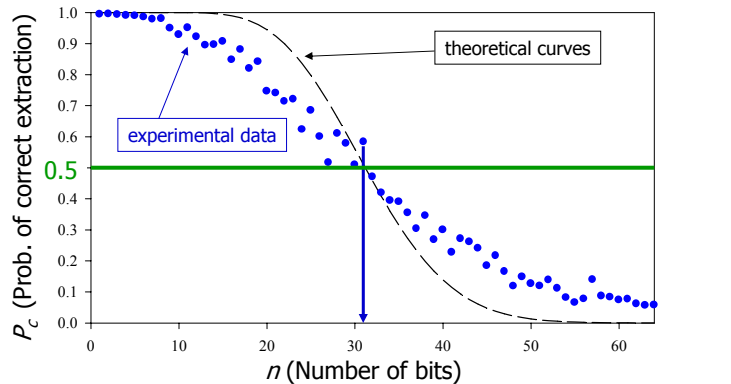
## Theoretical analysis

- WM strength (experimental results)
  - 36.619 (not compressed)
  - 18.663 (JPEG compressed : “worst acceptable quality”)



## Experimental results: prob. of correct extraction

- Prob. of correct extraction after JPEG compression



experimental capacity = 30/31 bits

$n = 30, P_{cd} = 0.509$   
 $n = 31, P_{cd} = 0.583$   
 $n = 32, P_{cd} = 0.470$

## Overview

- Background & aim of this study
- Problem definition
- Theoretical analysis on capacity
- Experiments
- **Conclusion & future works**

## Conclusion & future works

- “Practical” capacity can be determined if
  - WM algorithm
  - limitationare given
- Future works
  - Application to other WM algorithms
  - Relation with channel capacity

Questions, comments, etc..



[sugiryo@jp.ibm.com](mailto:sugiryo@jp.ibm.com)

## Backup sheets

- Backup Sheets from here

**BACKUP**

## Too little capacity?

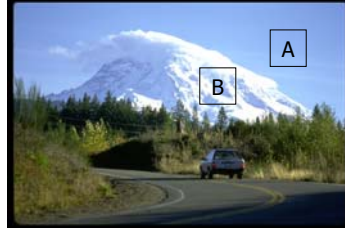
- Depends on WM algorithm
  - How much WM degrades by a certain compression?
- Capacity would be larger if
  - WM is more robust against compression
  - The requirements on reliability is more tolerant

## Patchwork algorithm

- First introduced by W.Bender et al., 1994

- Embedding

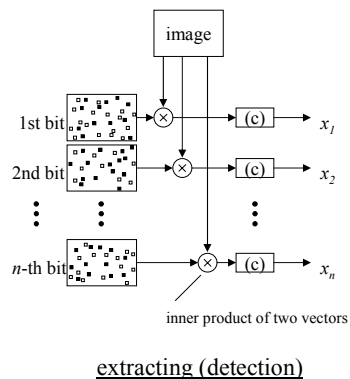
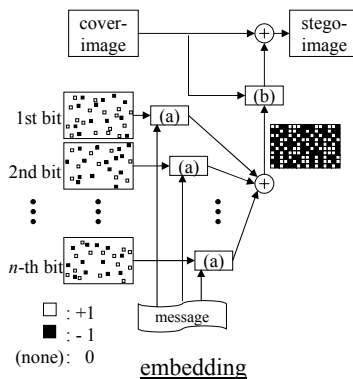
- embed "1":
  - brighten patch A
  - darken patch B
- embed "0":
  - the opposite



- Detecting

- $s = \Sigma(a_i - b_i)$ ,
- detect "0", if  $s < -T$
- not detect, if  $-T < s < T$
- detect "1", if  $s > T$

## Modified patchwork algorithm



- if  $(message)_i = "0"$ , swap  and  for  $i$ -th bit  
(no change if  $(message)_i = "1"$ )
- transparency control
- normalization

## Assumptions on WMing scheme (4)

- $\mu$  is assumed to be proportional to  $\sqrt{1/n}$

## Measurement of WM strength

- "WM strength" = "Detection value when assuming 1bit embedding"
- Actually, the detection value is in proportion to  $\sqrt{1/n}$  (n: number of bits)
- e.g.)  $n=12$ , (detection value)=3.5  
(WM strength) =  $3.5 \times \sqrt{12} = 12.12$

**Cover-image (before embedding)**



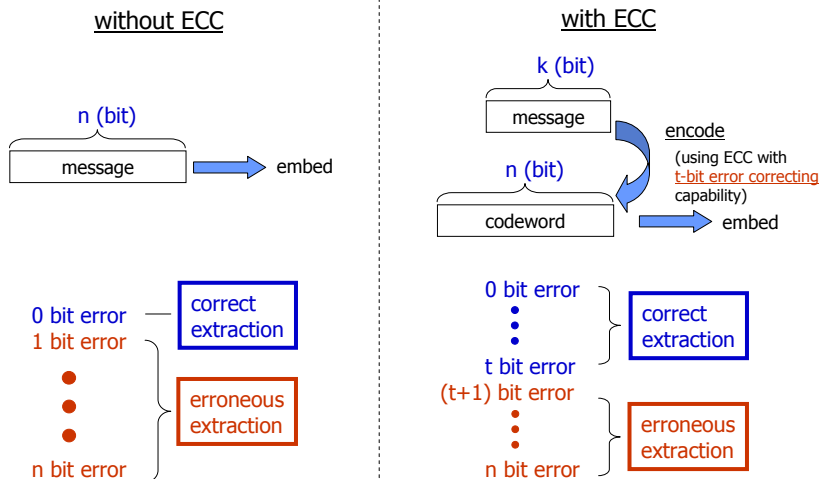
**Stego-image (after embedding)**



## Experiment - Conditions -

- Constraints:  $P_{fp} < 10^{-6}$ ,  $P_{be} < 10^{-4}$ ,  $P_{cd} > 0.5$
- Limit of degradation: JPEG compression (Quality=80)
- Tested on Patchwork-based algorithm
  - “Patchwork algorithm” (W.Bender et al., 1994)
  - Modified it for multiple-bit embedding
    - simply divided the image by the number of bits
- 1000 images (640 x 426)

## Employing ECC (1)



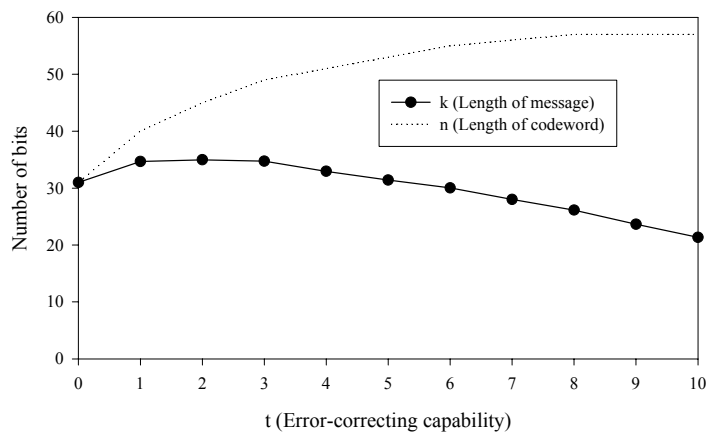
## Employing ECC (2)

- Hamming bound
  - for  $(n,k,t)$  linear block code ( $q$ : number of symbols,  $q=2$  in this case)

$$n - k \geq \log_q \left\{ \sum_{i=0}^t \binom{n}{i} (q-1)^i \right\}$$

## Employing ECC (3)

- Maximum  $k$  @  $t=2$  (approx. 35 bits)



## Old sheets

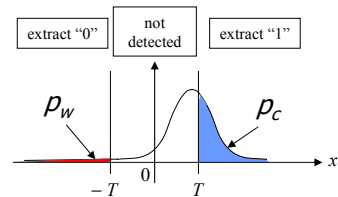
- Old Sheets from here

OLD

## Formulation of reliability

### Basic Formulae

- If  $x_i$  follows  $N(\mu, 1)$ .....
- For  $i$ -th bit
  - Prob. of correct extraction
  - Prob. of wrong extraction
- For  $n$  bits
  - Prob. of  $i$ -bit error extraction (out of  $n$  bits)



$$p_c = \int_T^{+\infty} f_{\mu,1}(x) dx$$

$$p_w = \int_{-\infty}^{-T} f_{\mu,1}(x) dx$$

$$p_e(i) = \binom{n}{i} \{p_w\}^i \{p_c\}^{n-i}$$

The message is assumed to be "11...11"

$f_{\mu,1}(x)$ : Normal dist. with mean  $\mu$ , variance 1  
 $N(\mu, 1)$

## Formulation of reliability (2)

### For non-WMed image

- $x_i$  follows  $N(0,1)$

- For  $i$ -th bit

– Prob. of detection

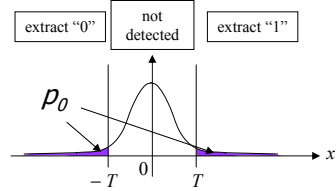
$$p_0 = \int_{-\infty}^{-T} f_{0,1}(x)dx + \int_T^{+\infty} f_{0,1}(x)dx$$

$$= \operatorname{erfc}\left(\frac{T}{\sqrt{2}}\right)$$

- For  $n$  bits

– Prob. of detection (false alarm)

$$P_{fp} = \{p_0\}^n$$



## Formulation of reliability (3)

### For WMed image

- $x_i$  follows  $N(\mu, 1)$  ( $\mu_{min} < \mu < \mu_{max}$ )

- For  $n$  bits

– Prob. of correct extraction

$$P_{cd} = p_e(0)$$

– Prob. of wrong extraction  
(erroneous extraction)

$$P_{be} = \sum_{i=1}^n p_e(i)$$

$p_e(i)$  : Prob. of  $i$ -bit error detection out of  $n$  bits

## Calculate threshold

- $T_{fp}$

- for satisfying  $P_{fp} < P_{fpmax}$
- can be solved analytically:

$$T_{fp} = \sqrt{2} \operatorname{erfc}^{-1} \left\{ \left\{ \frac{P_{fpmax}}{P_0} \right\}^n \right\}$$

$$P_{fp} = \{p_0\}^n$$

$$p_0 = \operatorname{erfc} \left( \frac{T}{\sqrt{2}} \right)$$

- $T_{be}$

- for satisfying  $P_{be} < P_{bemax}$
- cannot be solved analytically
  - numerically solved by Newton method
- $T_{be}$  depends on  $\mu$

$$P_{be} = \sum_{i=1}^n p_c(i)$$

$$p_c(i) = \binom{n}{i} \{p_w\}^i \{p_c\}^{n-i}$$

$$p_w = \int_{-\infty}^T f_{\mu,1}(x) dx \quad p_c = \int_T^{\infty} f_{\mu,1}(x) dx$$

- $T$

- Both of the constraint must be satisfied at the same time

$$T = \max_{0 \leq \mu \leq \mu_{max}} (T_{fp}, T_{be}(\mu))$$