

## 정보은닉 기술과 디지털 컨텐츠 보호

- Information Hiding for Secure Digital Contents -

2001. 6. 2.

이형우 (천안대 학교)

## Information Hiding ?

Who wrote the works ?



William Shakespeare



Francis Bacon

? *Daffodilus, son*  
→ *88546112*  
F S ST ALBAN

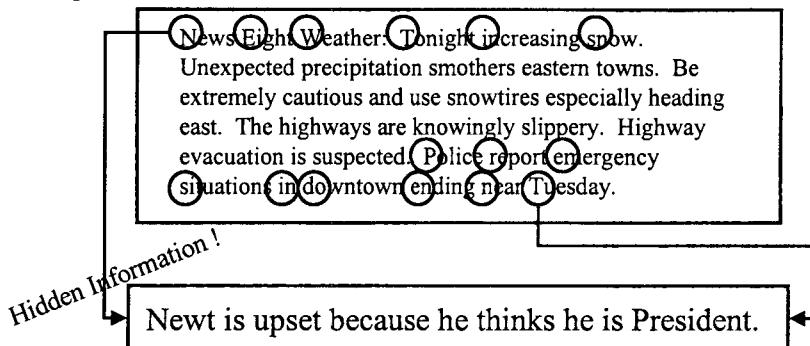
One is a country boy from Stratford; the other a titled, educated gentleman.

Are There Ciphers in Shakespeare?  
by Penn Leary.

## What is Information Hiding ?

### □ Simple Example 1

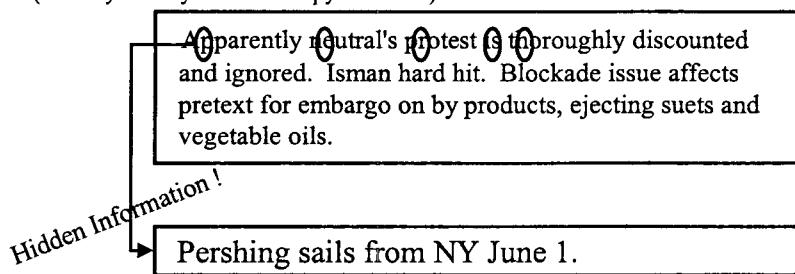
Taking the first letter in each word



## What is Information Hiding ?

### □ Simple Example 2

Taking the second letter in each word  
(actually sent by a German Spy in WWII)



## What is Information Hiding ?

### □ Simple Example 3

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.

Sentence S0

Overlap S0 + S1

We **explore** new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.

We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet.

Hidden Information!

explore the world wide web

Sentence S1

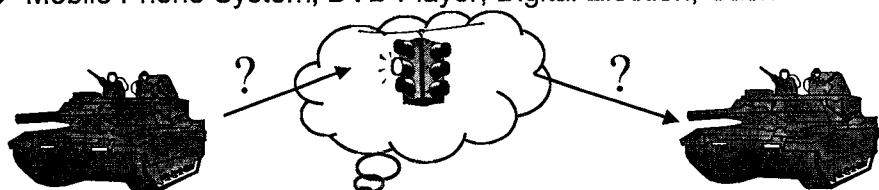
## Information Hiding

### □ Distinguished but imperceptible marks

- ❖ Contain a hidden copyright notice or serial number
- ❖ Help to prevent unauthorized copying directly

### □ Example

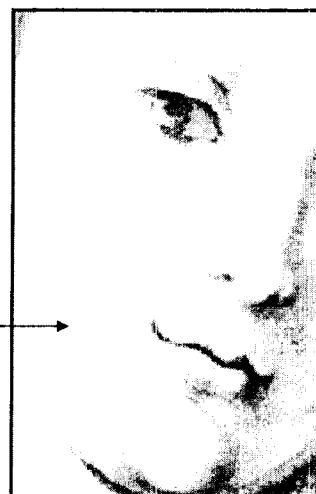
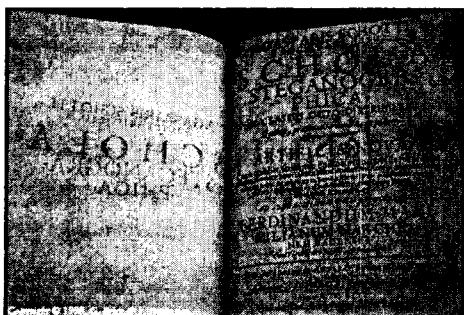
- ❖ Military Communications System
  - Conceal its sender, its receiver or its very existence
- ❖ Mobile Phone System, DVD Player, Digital Election, Cash



## **Steganography : Information Hiding**

### **□ Steganographia (Secret Writing), by Johannes Trithemius. 1500.**

- ❖ a system of angel magic
- ❖ a method of sending messages without symbols or messenger



2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

7

## **Steganography : Information Hiding**

### **□ Steganography conceals the fact that a message is being sent !**

### **□ Steganography**

- ❖ “covered writing”
- ❖ methods of secret communications that conceal the very existence of the message
  - covert channels
  - spread spectrum communication
  - invisible inks

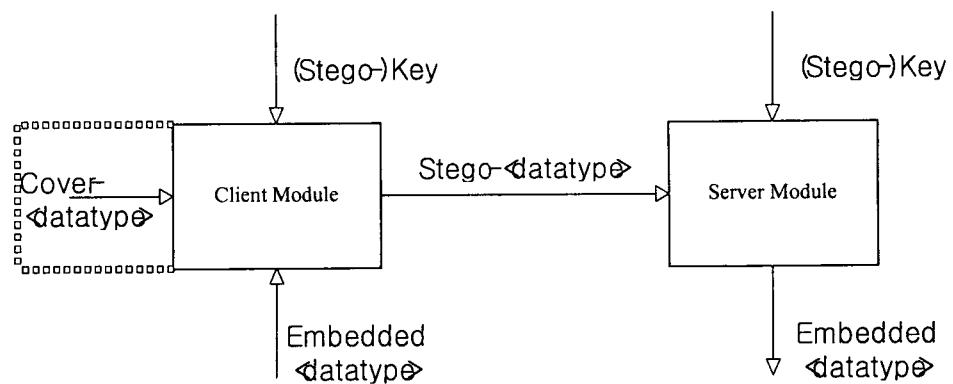
2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

8

## **Steganography : Information Hiding**

### **□ Steganographic Model**

- ❖ Cover Data / Embedded Data



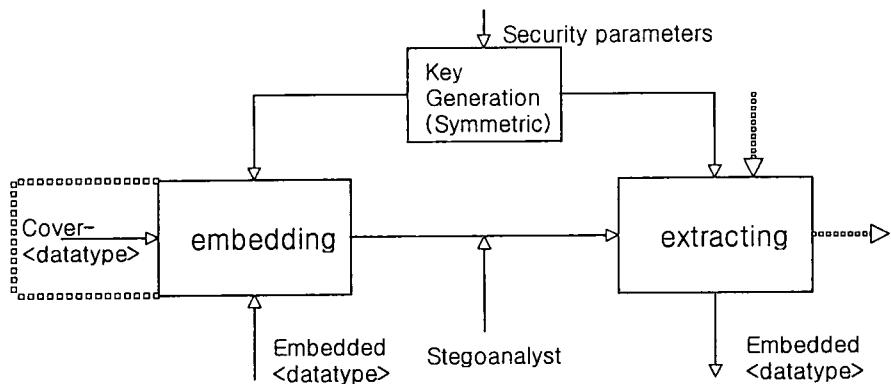
2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

9

## **Steganography : Information Hiding**

### **□ Key based Steganographic Model**

- ❖ Symmetric Stego Key



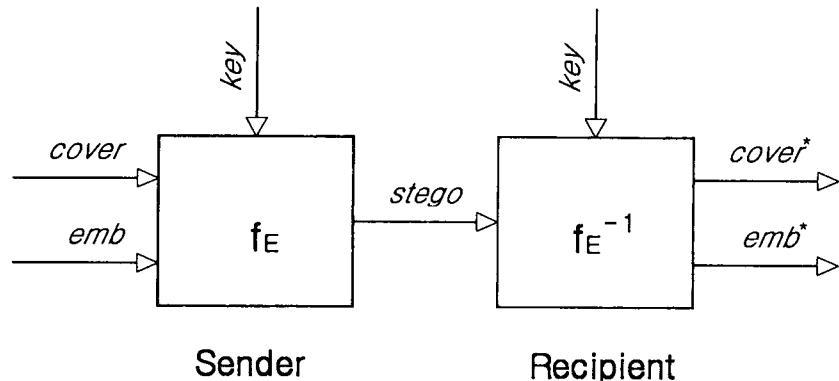
2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

10

## Steganography : Information Hiding

### □ Steganographic Function $f_E$

❖ Cover Data / Embedded Data / Stego Data / Stego Key

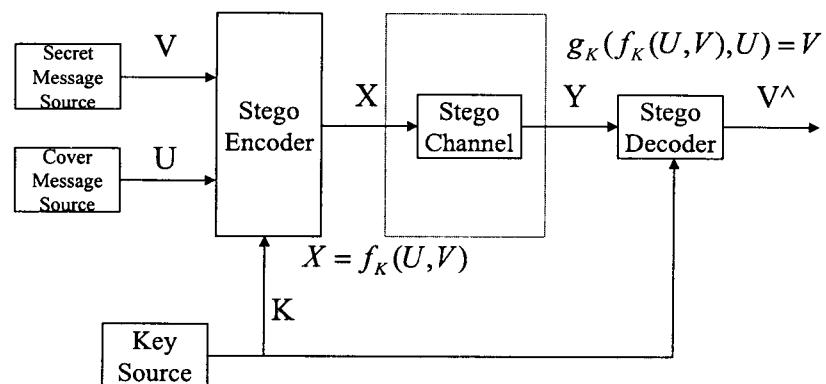


2001 멀티미디어 학회 춘계학술대회, 유토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

11

## General Model of Information Hiding

### □ General Model for Information Hiding



2001 멀티미디어 학회 춘계학술대회, 유토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

12

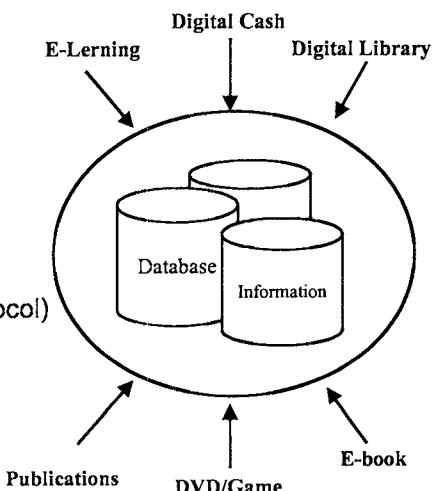
## Digital Electronic Commerce : D-Commerce

### □ Digital Commerce

- ❖ Publications
- ❖ Digital TV, DVD
- ❖ Digital Information(Digital Library)
- ❖ Game
- ❖ Music/Image/Movie
- ❖ E-Book(Digital Book)
- ❖ Cyber Education(E-Learning)
- ❖ Digital Cash(Electronic Payment Protocol)

### □ Core

- ❖ Digital Contents (eContents)



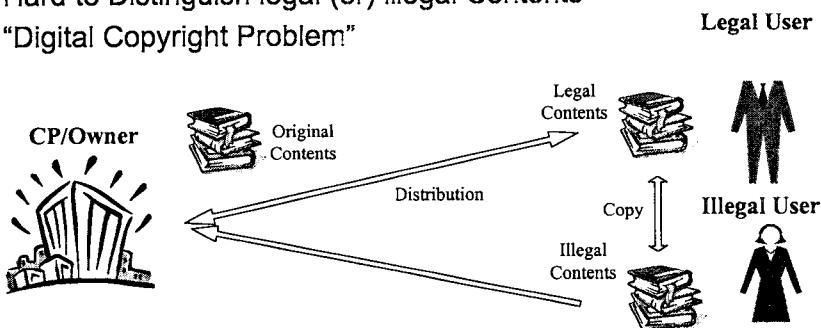
2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

13

## Properties of Digital Contents

### □ Digital Contents

- ❖ Easy to Copy
- ❖ Easy to Distribute
- ❖ Hard to Distinguish legal (or) illegal Contents
- ❖ "Digital Copyright Problem"



2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

14

89

## Let's Embed the Copyright Message

### □ Copyright

- ❖ Digital Mark
- ❖ Digital Ownership

### □ “Copyright Hiding” in Digital Contents

- ❖ Digital Object Identifier (DOI) Hiding
- ❖ Digital (Copy)Right Management
- ❖ Copyright Information Hiding !



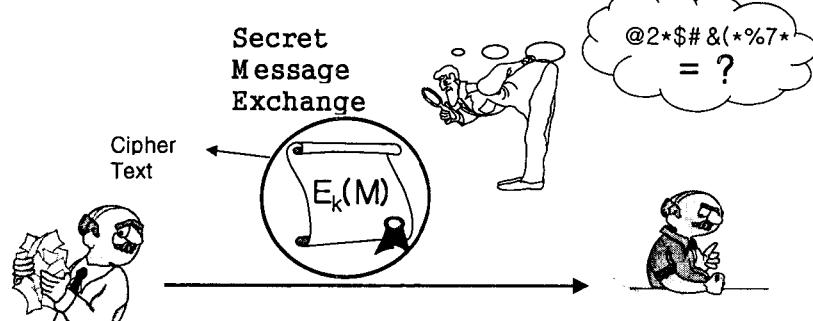
2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

15

## Cryptography : Information Security

### □ Cryptography

- ❖ “Secret Writing”
- ❖ “Secret Channel of Secret Message”



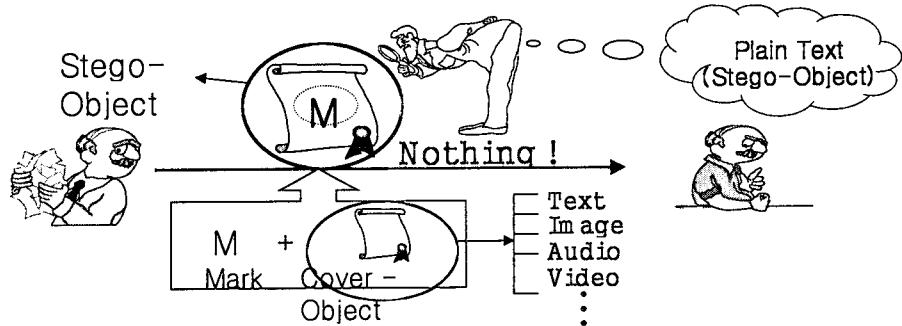
2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

16

## Steganography : Information Hiding

### □ Steganography

- ❖ “Covered Writing”
- ❖ “Hiding of Message” & “Conceals the very existence of the secret message”

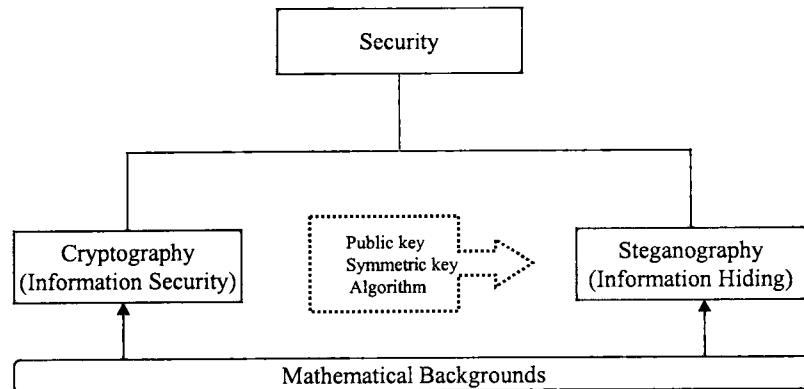


2001 멀티미디어 학회 춘계학술대회, 뮤토리얼·정보윤닉 기술과 디지털 컨텐츠 보호

17

## Relationship & New Paradigm

### □ Security Paradigm

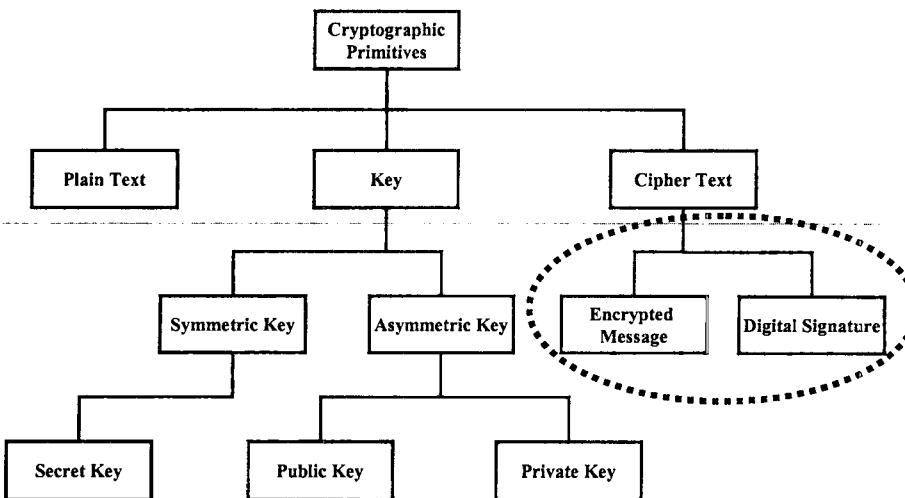


2001 멀티미디어 학회 춘계학술대회, 뮤토리얼·정보윤닉 기술과 디지털 컨텐츠 보호

18

91

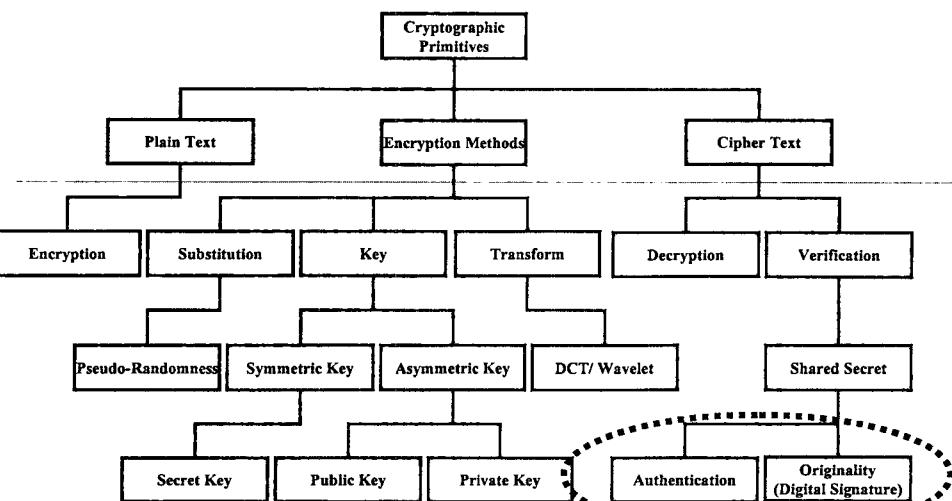
## Cryptographic Primitives



2001 멀티미디어 학회 춘계학술대회, 투토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

19

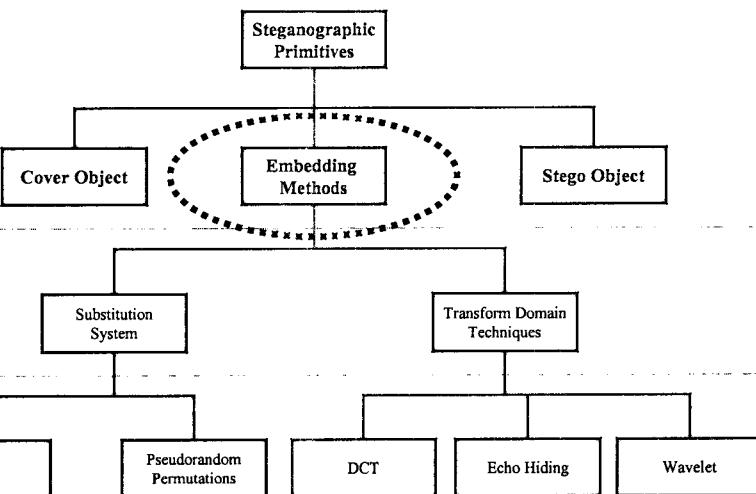
## Cryptographic Primitives



2001 멀티미디어 학회 춘계학술대회, 투토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

20

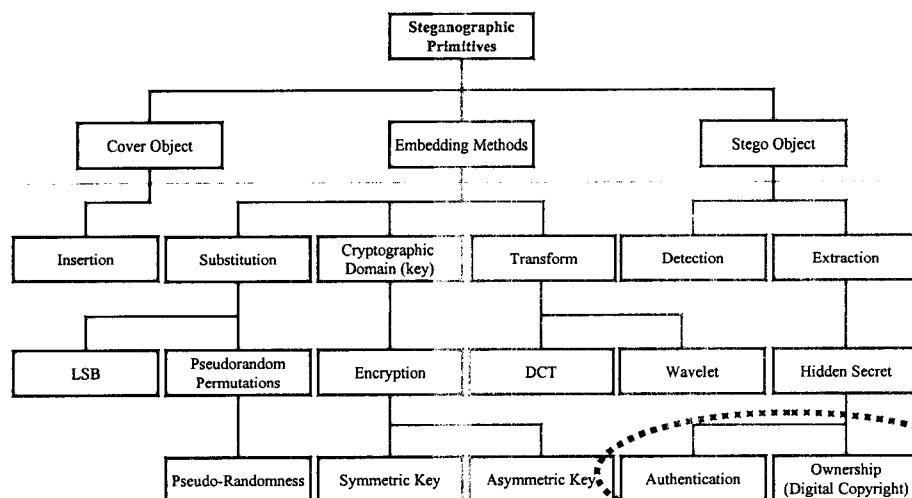
## Steganographic Primitives



2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

21

## Steganographic Primitives

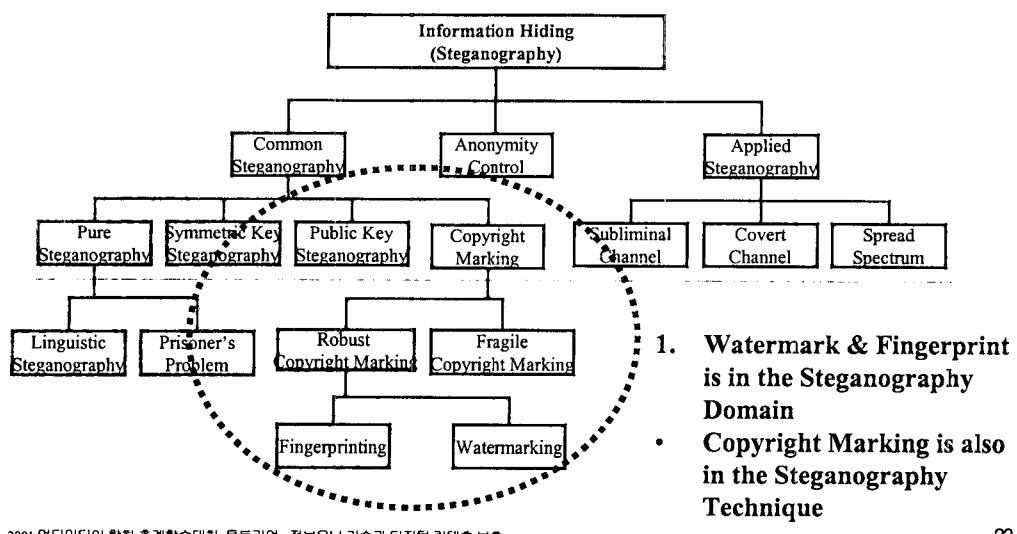


2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

22

93

## Steganography Paradigm

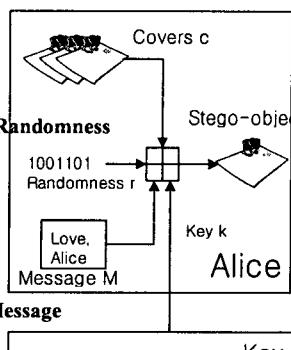


2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

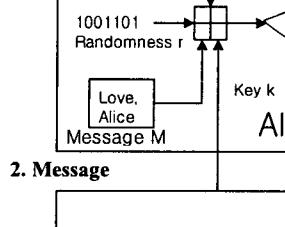
23

## Steganography : Model & Considerations

### 1. Cover Selection



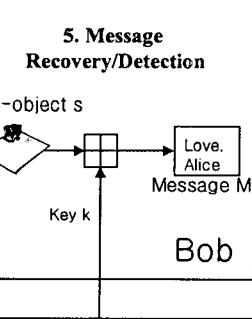
### 3. Pseudo-Randomness



### 2. Message

Key Generation facility

### 4. Attack



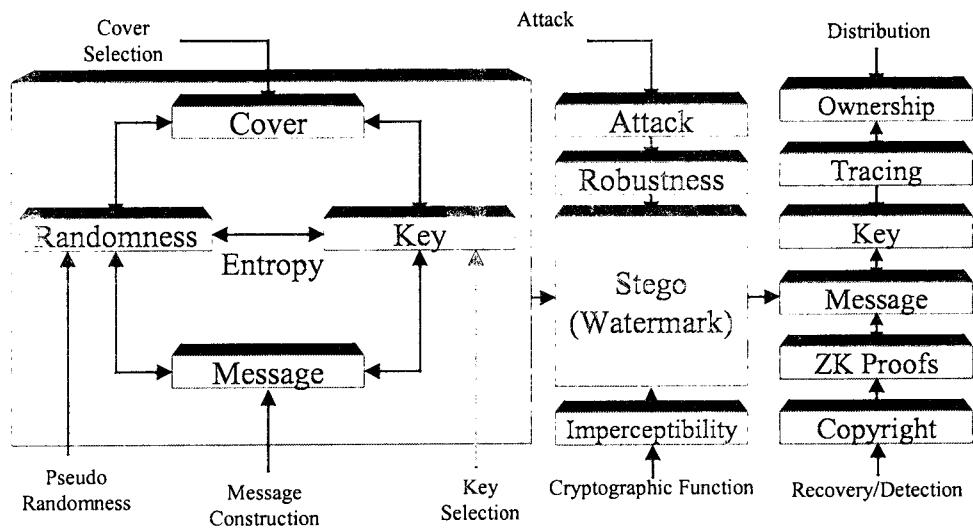
### 5. Message Recovery/Detection

Key Generation facility

2001 멀티미디어 학회 춘계학술대회, 뮤토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

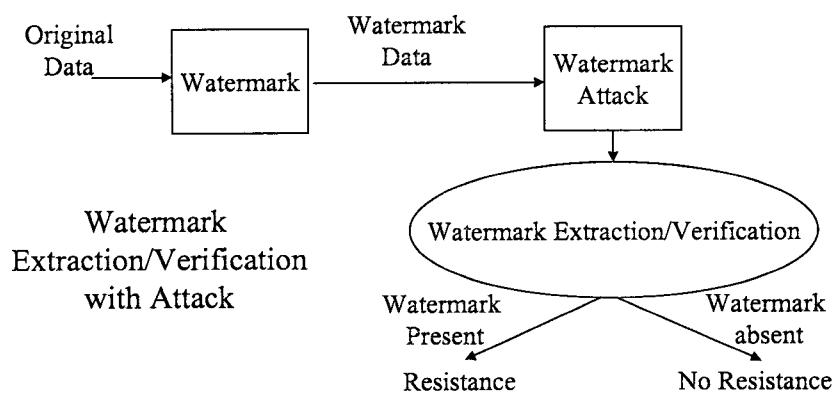
24

## Steganography : Detail Model



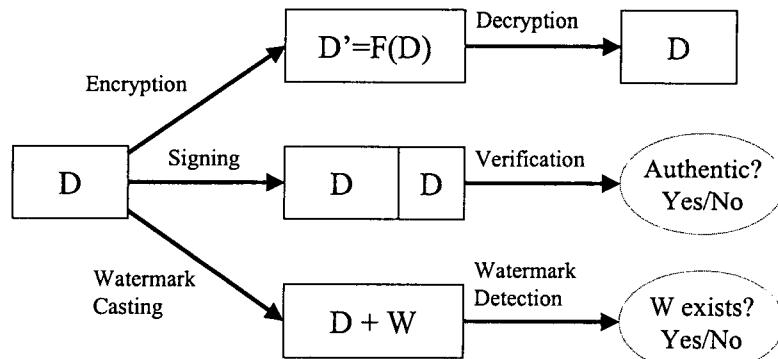
## Digital Watermarking

### □ Overall Model



## Digital Watermarking

### □ Crypto & Digital Watermarking



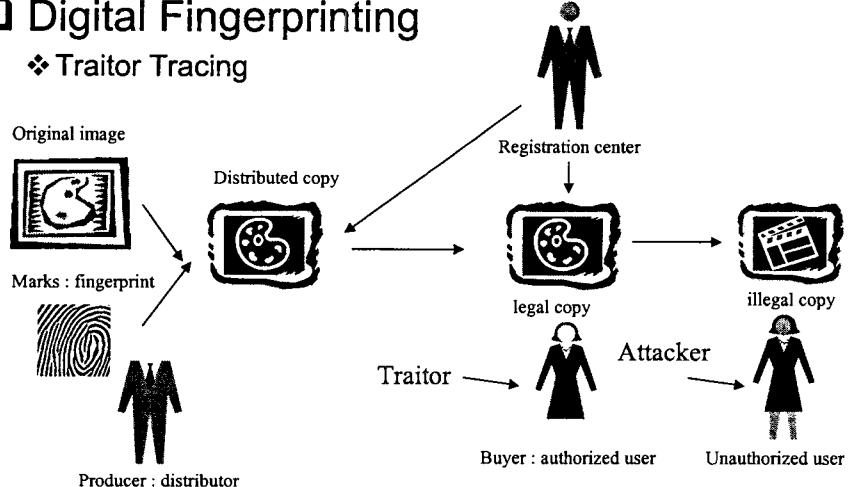
2001 멀티미디어 학회 총계학술대회, 뮤토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

27

## Digital Fingerprinting

### □ Digital Fingerprinting

#### ❖ Traitor Tracing



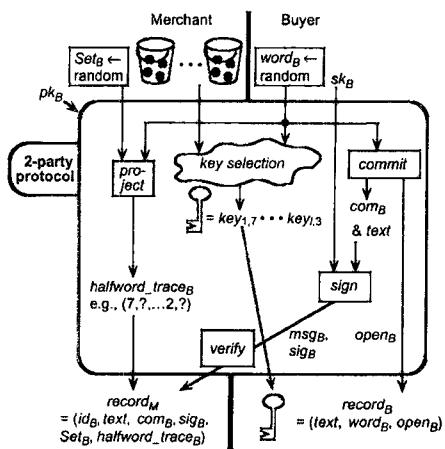
2001 멀티미디어 학회 총계학술대회, 뮤토리얼 : 정보온닉 기술과 디지털 컨텐츠 보호

28

## Digital Fingerprinting

### □ Asymmetric Fingerprinting

- ❖ Embedding Personal Information For Tracing



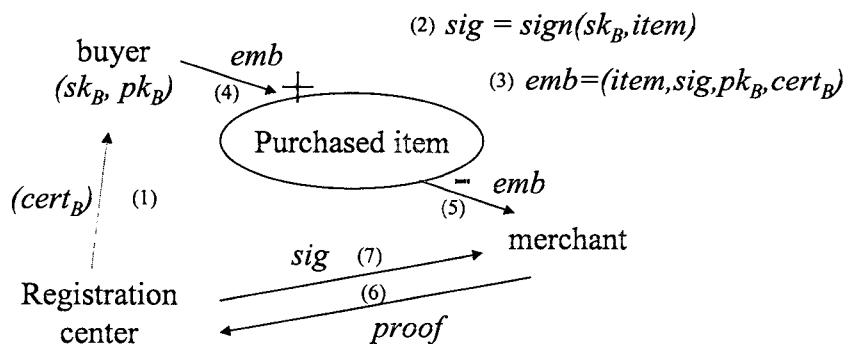
2001 멀티미디어 학회 춘계학술대회, 유토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

29

## Digital Fingerprinting

### □ Anonymous Fingerprinting

- ❖ Embedding Copyright Information for Tracing

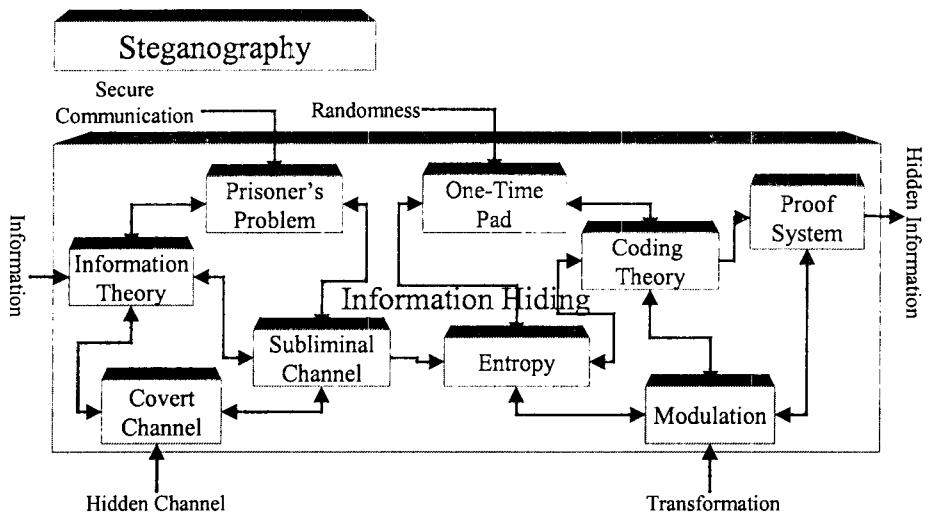


2001 멀티미디어 학회 춘계학술대회, 유토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

30

97

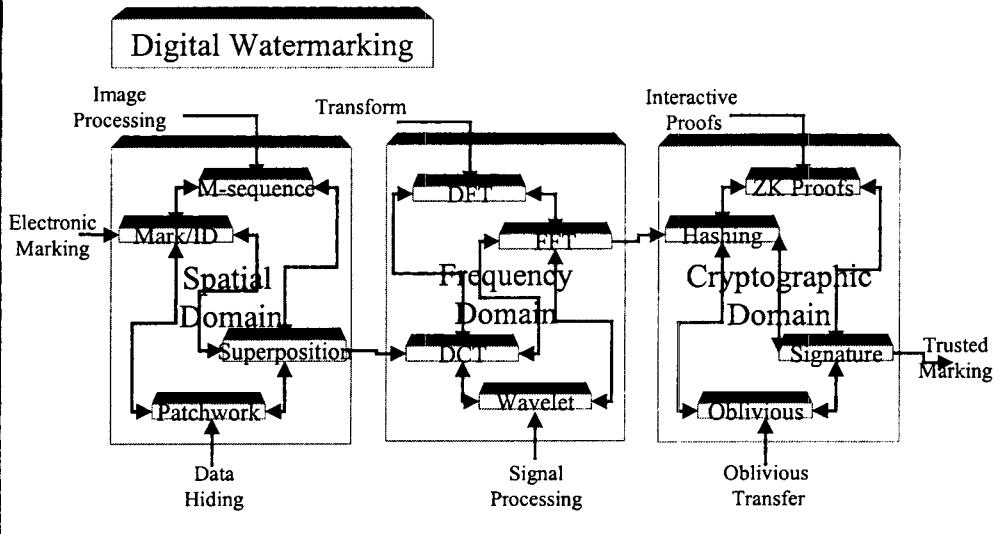
## Research Trends : Steganography



2001 멀티미디어 학회 춘계학술대회, 유토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

31

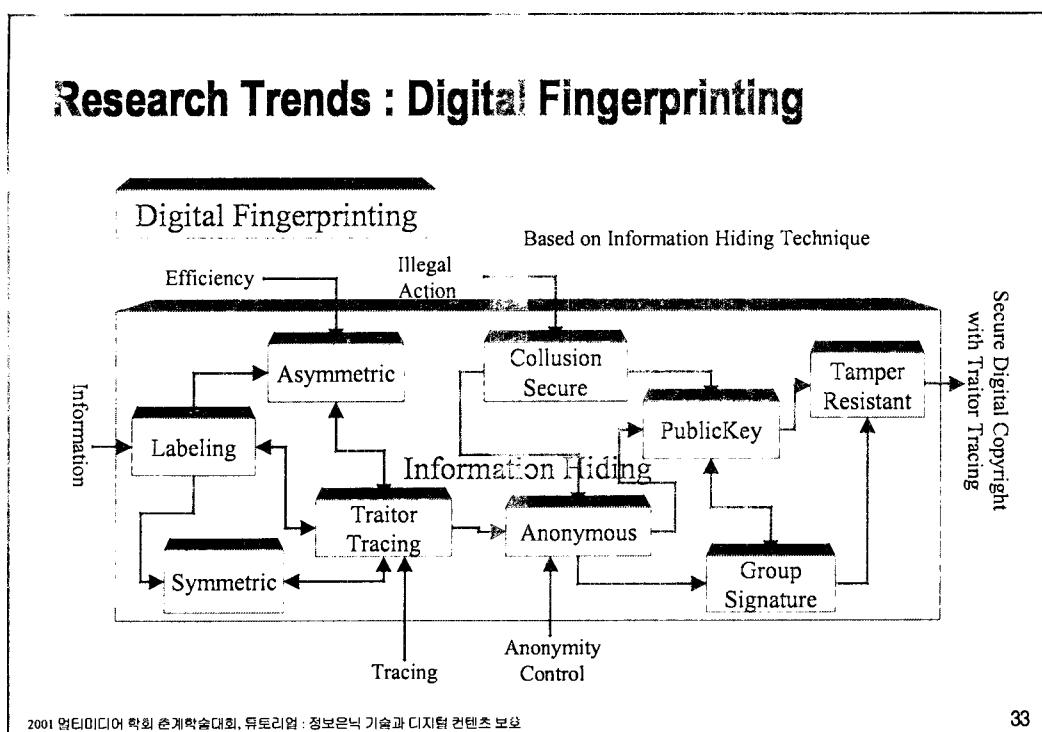
## Research Trends : Digital Watermarking



2001 멀티미디어 학회 춘계학술대회, 유토리얼 : 정보은닉 기술과 디지털 컨텐츠 보호

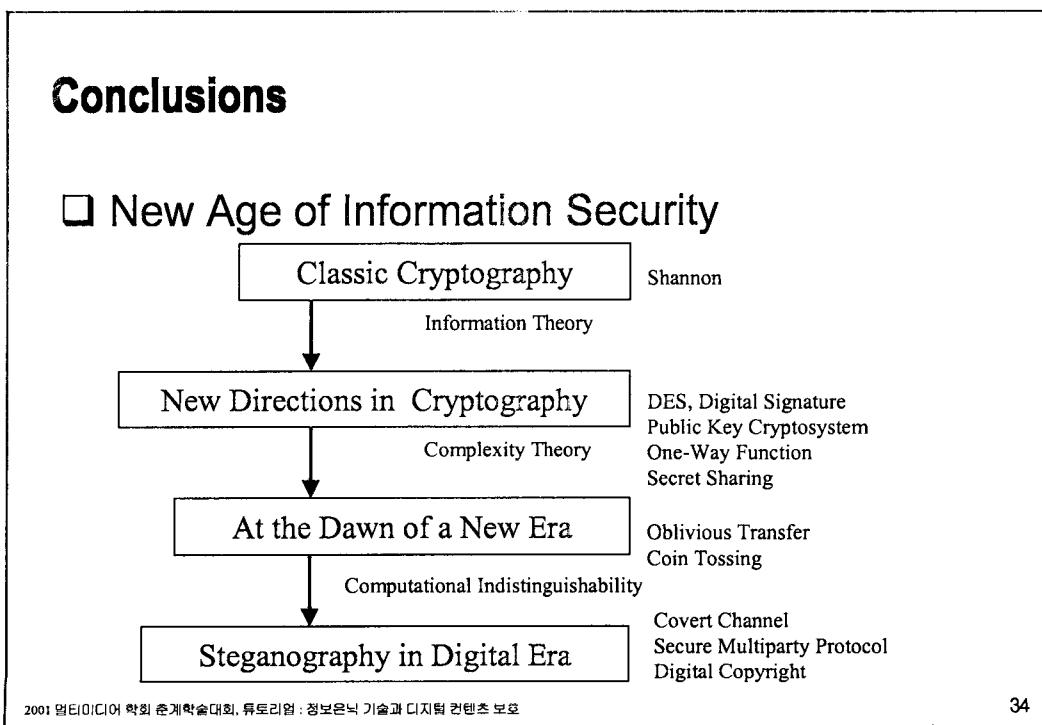
32

## Research Trends : Digital Fingerprinting



## Conclusions

### □ New Age of Information Security



**Thanks**



**Future Works : Steganographic Secure Digital Content  
Distribution Mechanism for “DRM” System ?**

**Hyung-Woo Lee  
ISEC Lab. Cheonan University  
hwlee@cheonan.ac.kr  
<http://infocom cheonan.ac.kr/~hwlee>**