KMMS 2001 Conf.

정보은닉 기술과 디지털 컨텐츠 보호

- Information Hiding for Secure Digital Contents -

2001. 6. 2.

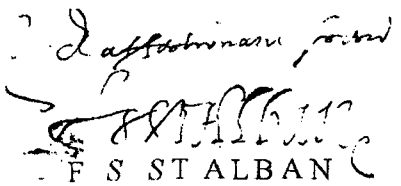
이형우 (천안대학교)

Information Hiding ?

❑ Who wrote the works ?

William Shakespeare

Francis Bacon



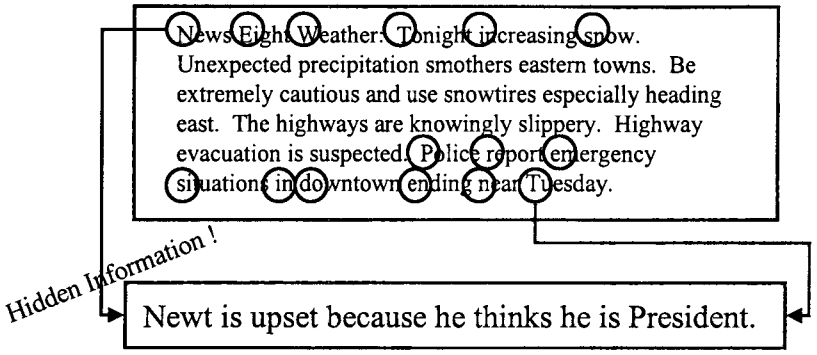
One is a country boy from Stratford; the other a titled, educated gentleman.

Are There Ciphers in Shakespeare?
by Penn Leary.

What is Information Hiding ?

❑ Simple Example 1

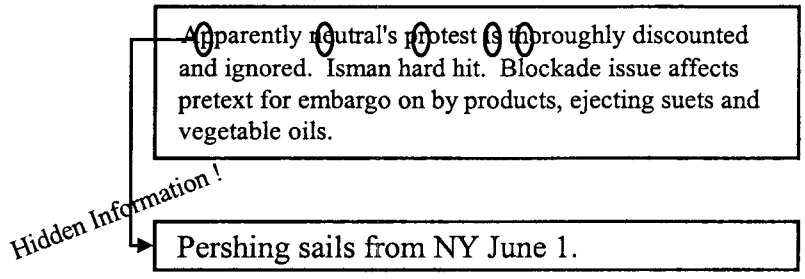
Taking the first letter in each word



What is Information Hiding ?

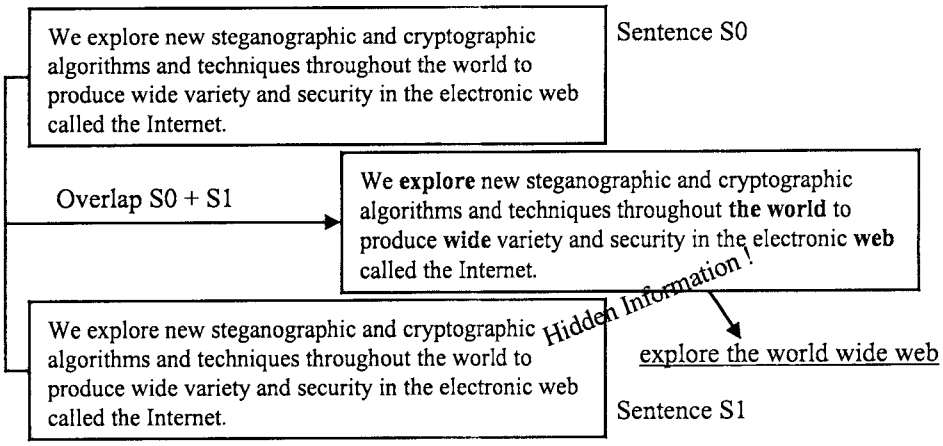
❑ Simple Example 2

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



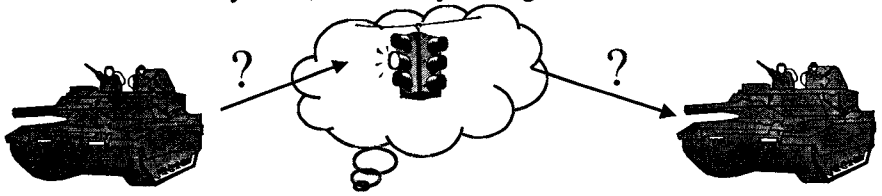
What is Information Hiding ?

- Simple Example 3



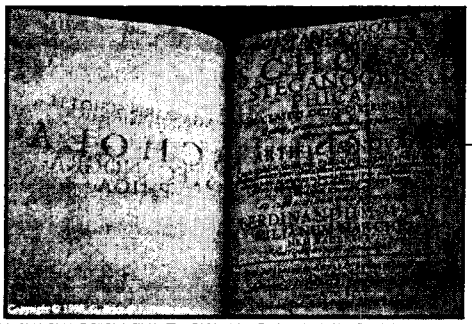
Information Hiding

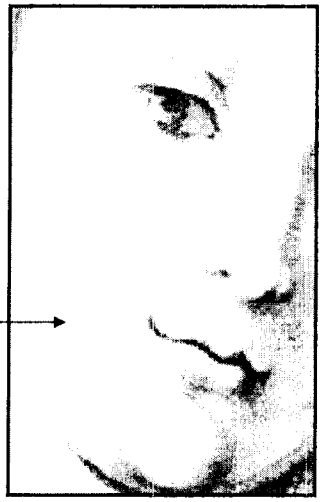
- Distinguished but imperceptible marks
  - Contain a hidden copyright notice or serial number
  - Help to prevent unauthorized copying directly
- Example
  - Military Communications System
    - Conceal its sender, its receiver or its very existence
  - Mobile Phone System, DVD Player, Digital Election, 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





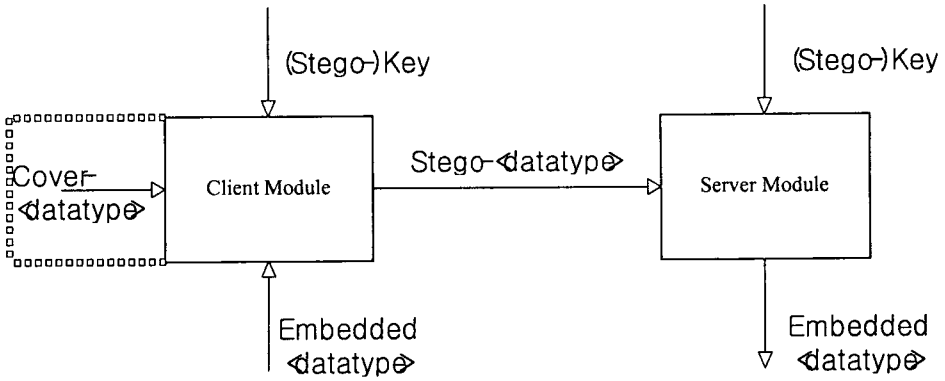
Steganography : Information Hiding

- 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

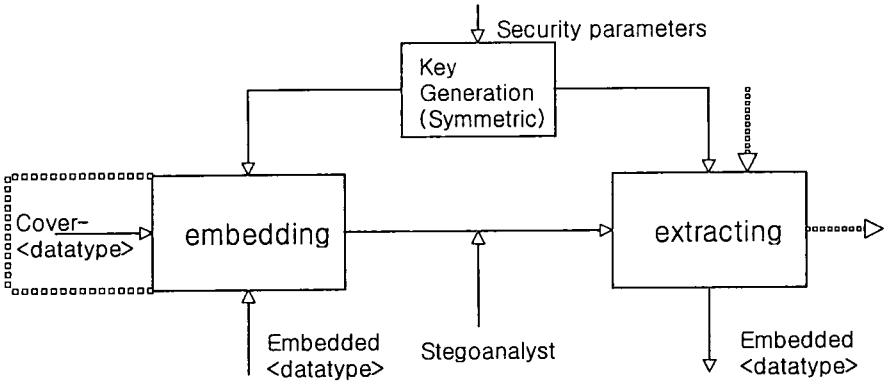
Steganography : Information Hiding

- Steganographic Model
  - Cover Data / Embedded Data



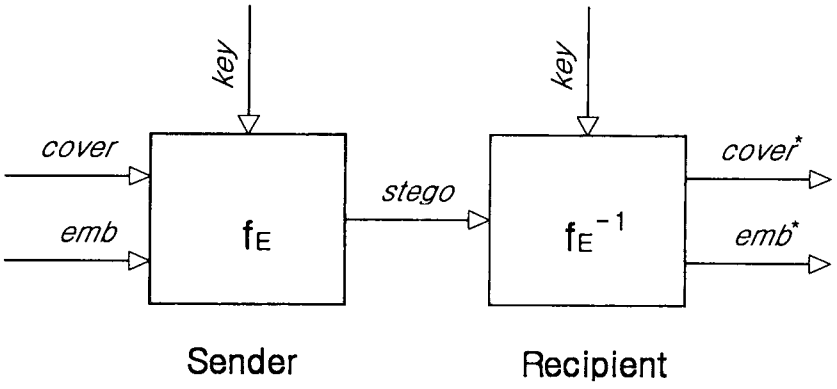
Steganography : Information Hiding

- Key based Steganographic Model
  - Symmetric Stego Key



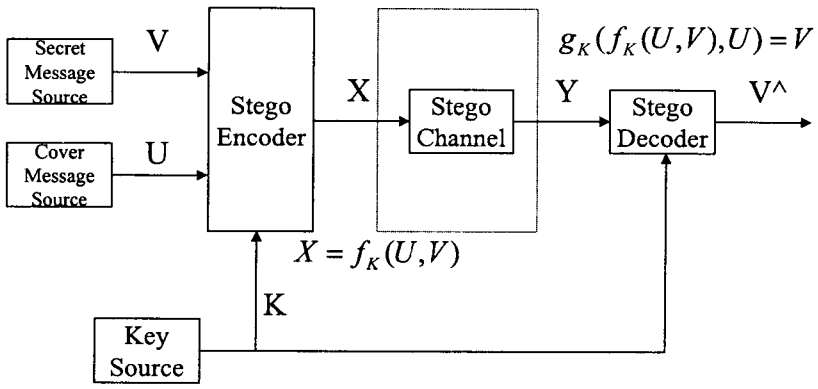
Steganography : Information Hiding

- Steganographic Function f_E
  - Cover Data / Embedded Data / Stego Data / Stego Key



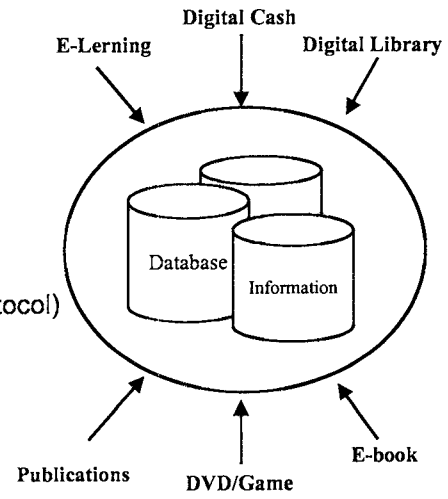
General Model of Information Hiding

- General Model for Information Hiding



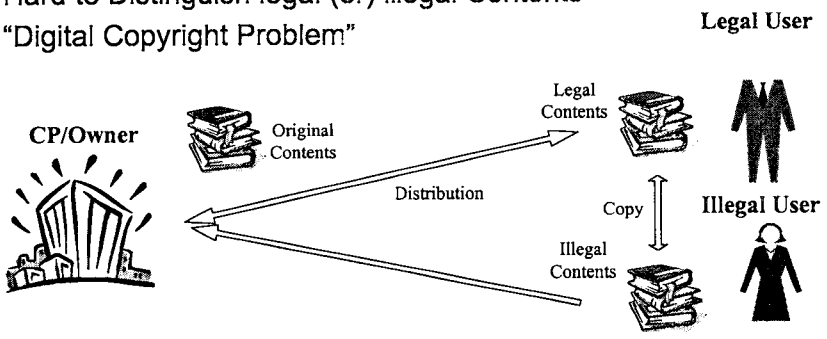
Digital Electronic Commerce : D-Commerce

- 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)



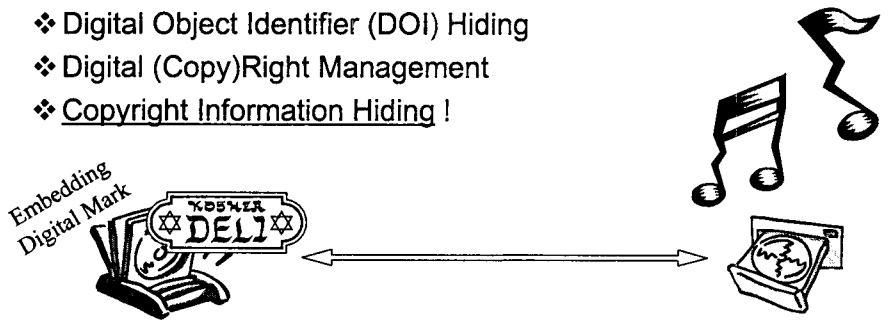
Properties of Digital Contents

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



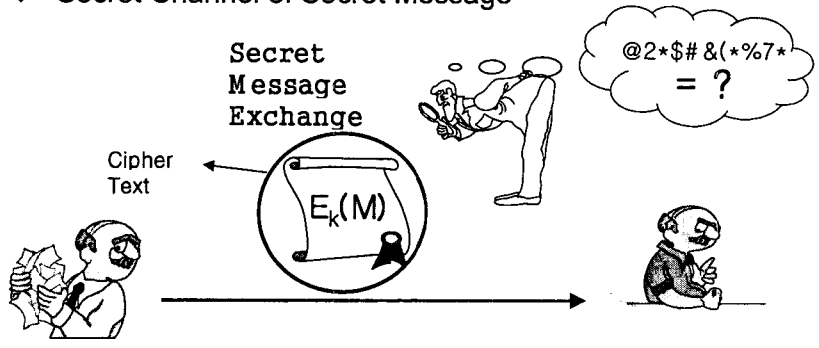
Let's Embed the Copyright Message

- Copyright
  - Digital Mark
  - Digital Ownership
- "Copyright Hiding" in Digital Contents
  - Digital Object Identifier (DOI) Hiding
  - Digital (Copy)Right Management
  - Copyright Information Hiding !



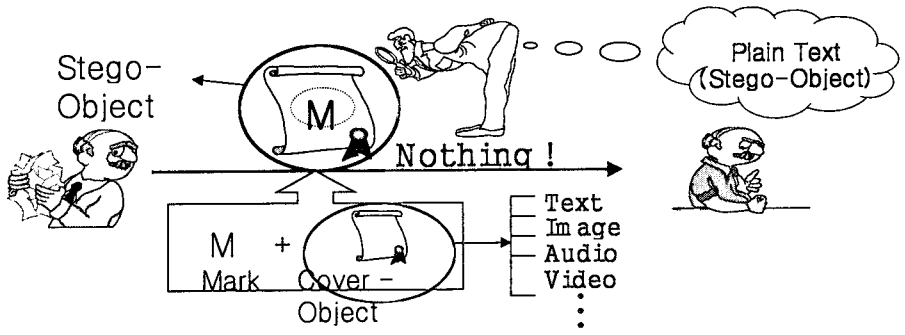
Cryptography : Information Security

- Cryptography
  - "Secret Writing"
  - "Secret Channel of Secret Message"



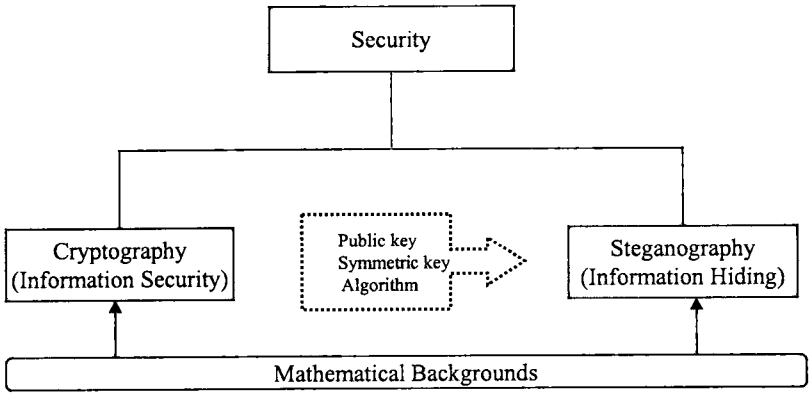
Steganography : Information Hiding

- Steganography
  - "Covered Writing"
  - "Hiding of Message" & "Conceals the very existence of the secret message"

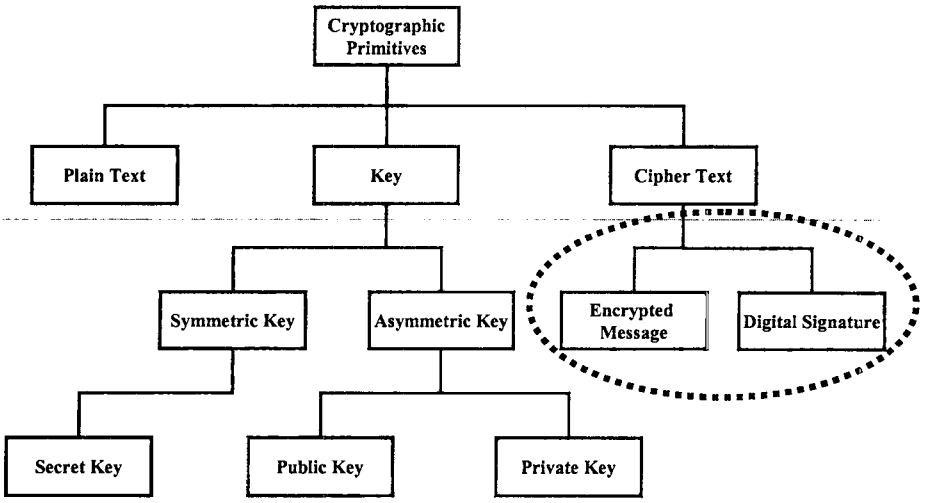


Relationship & New Paradigm

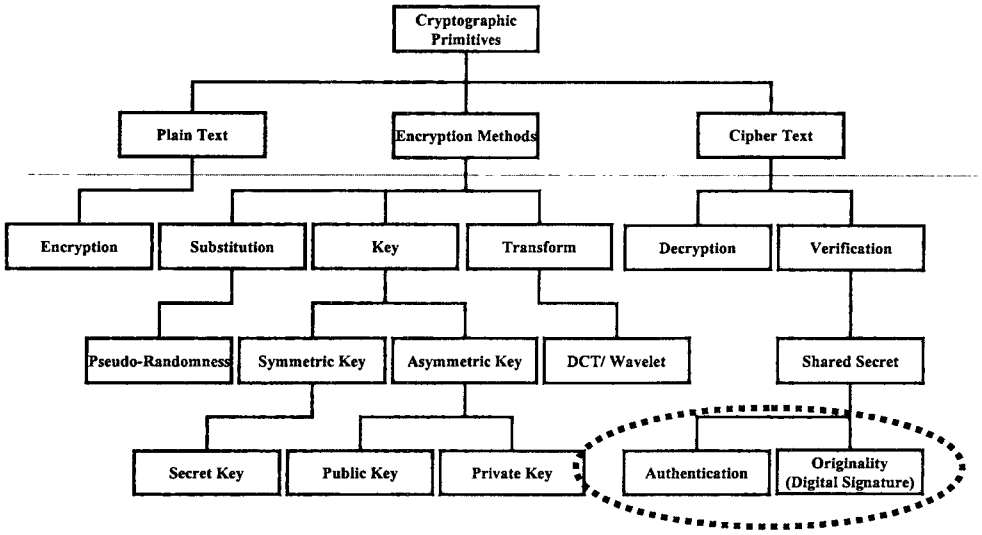
- Security Paradigm



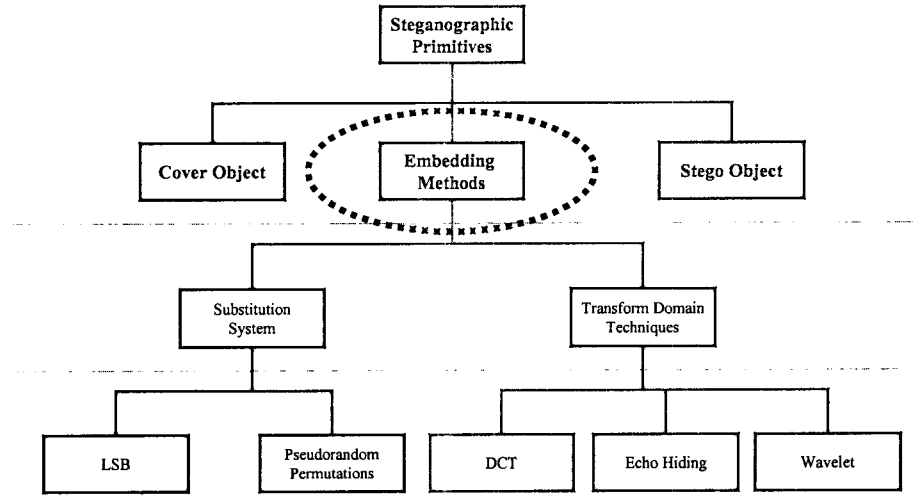
Cryptographic Primitives



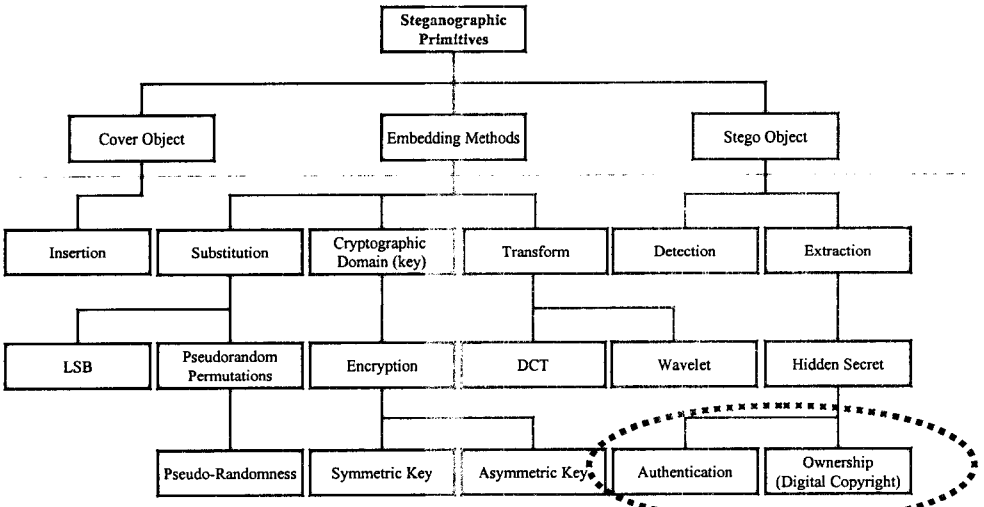
Cryptographic Primitives



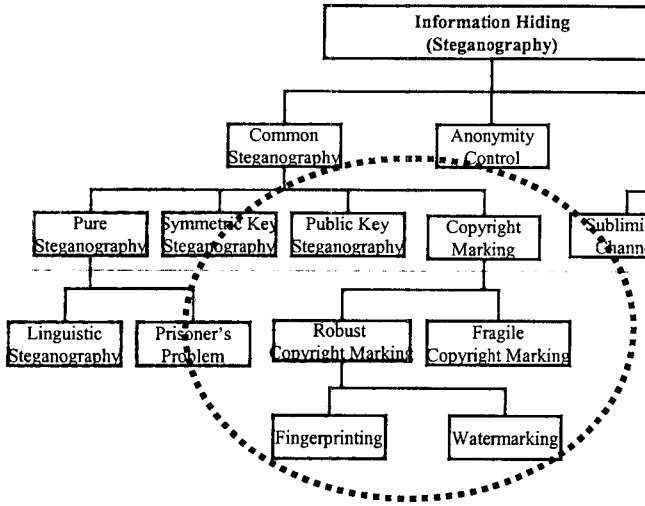
Steganographic Primitives



Steganographic Primitives

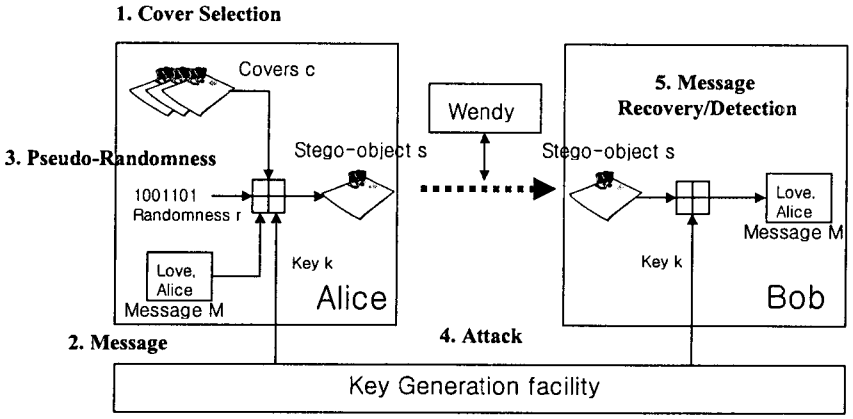


Steganography Paradigm

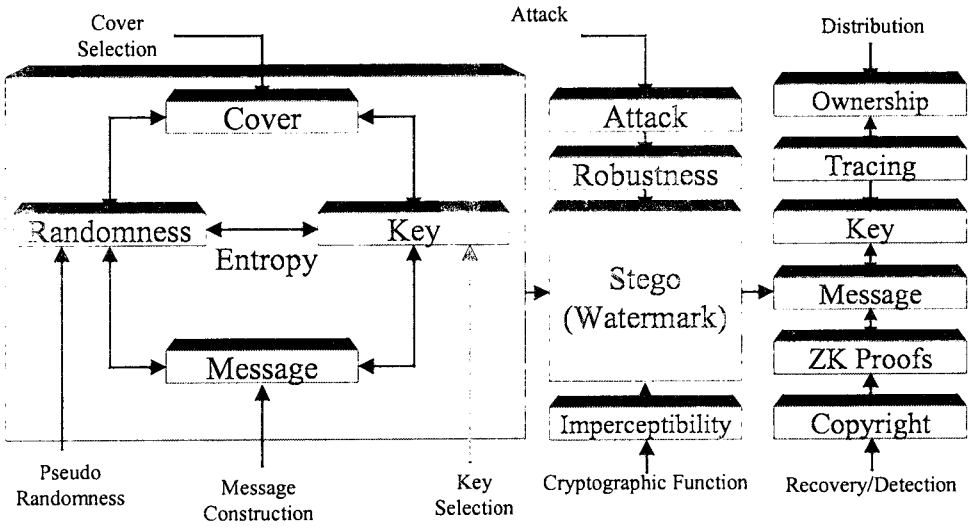


1. **Watermark & Fingerprint is in the Steganography Domain**
- **Copyright Marking is also in the Steganography Technique**

Steganography : Model & Considerations

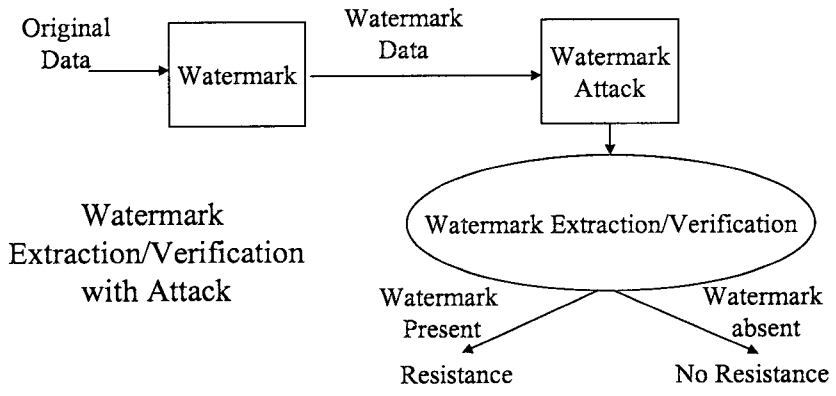


Steganography : Detail Model



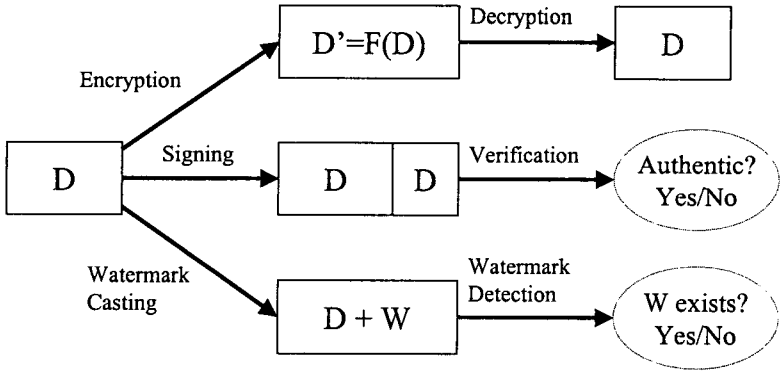
Digital Watermarking

❑ Overall Model



Digital Watermarking

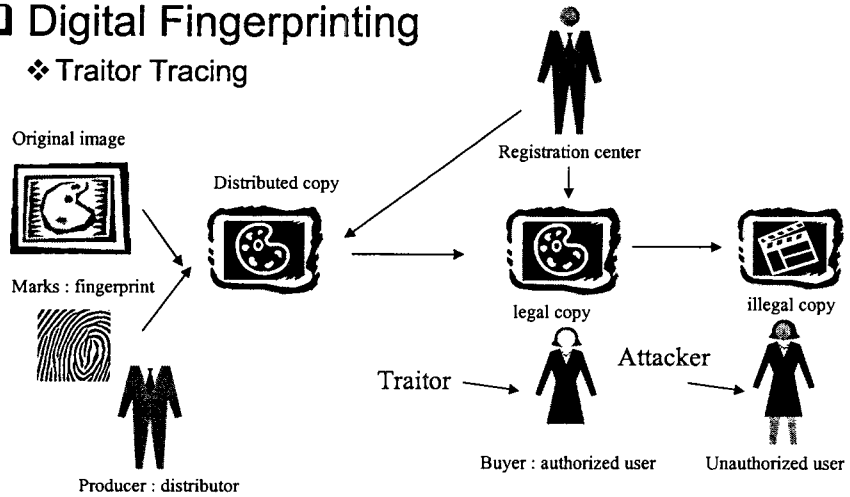
❑ Crypto & Digital Watermarking



Digital Fingerprinting

❑ Digital Fingerprinting

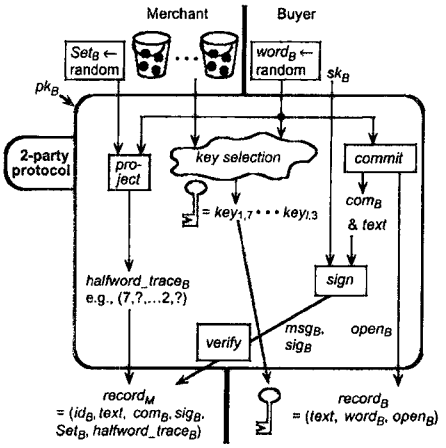
❖ Traitor Tracing



Digital Fingerprinting

❑ Asymmetric Fingerprinting

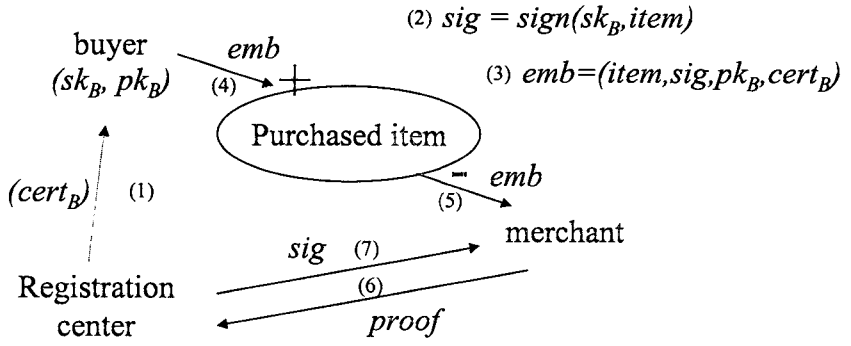
- ❖ Embedding Personal Information For Tracing



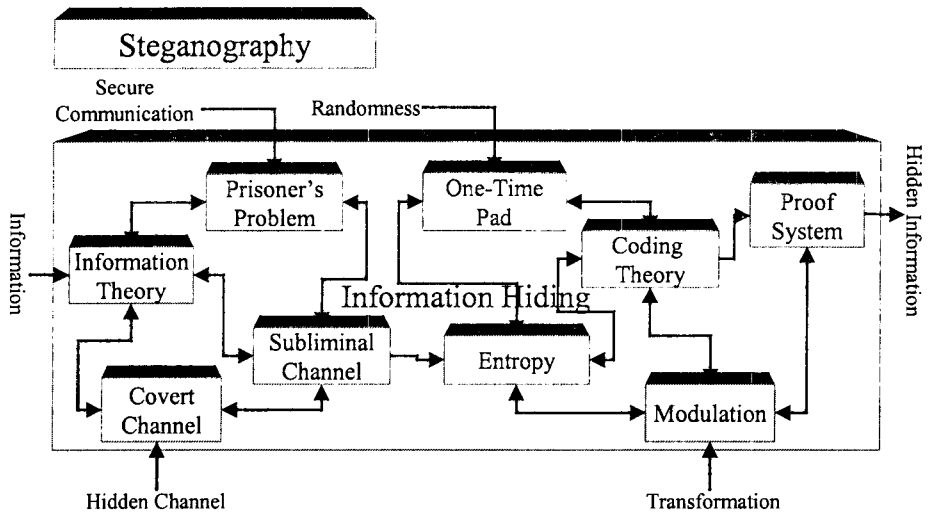
Digital Fingerprinting

❑ Anonymous Fingerprinting

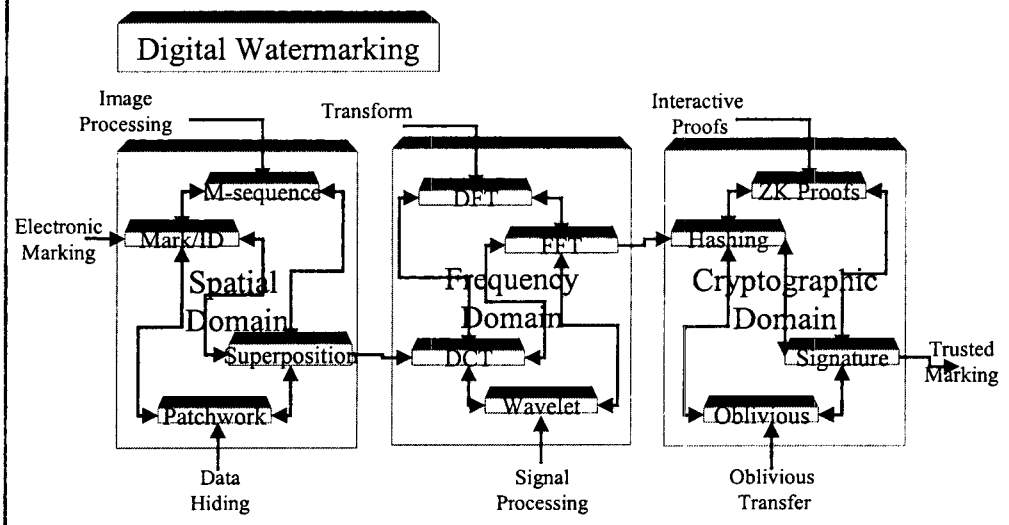
- ❖ Embedding Copyright Information for Tracing



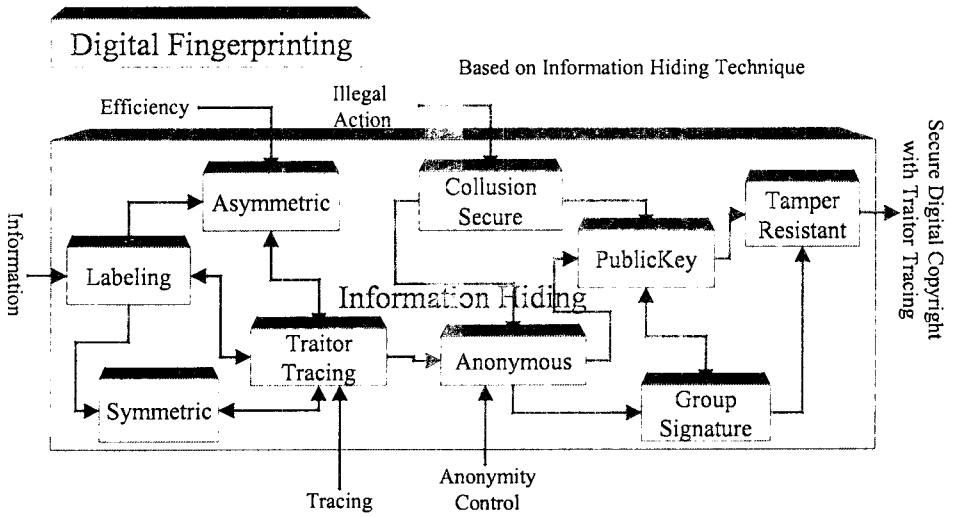
Research Trends : Steganography



Research Trends : Digital Watermarking

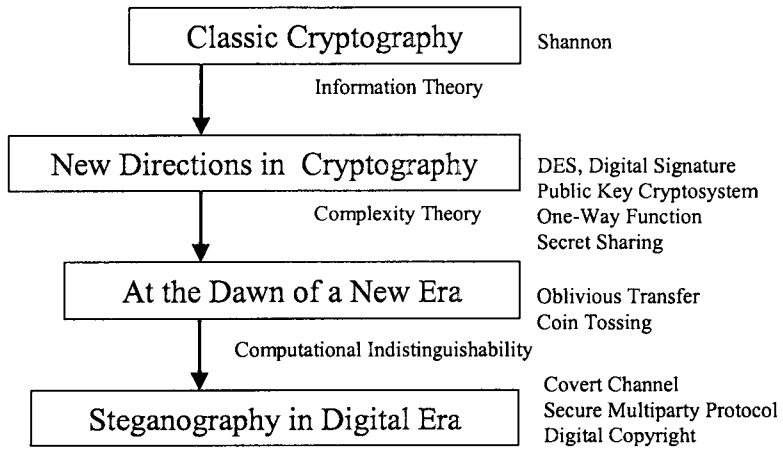


Research Trends : Digital Fingerprinting



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