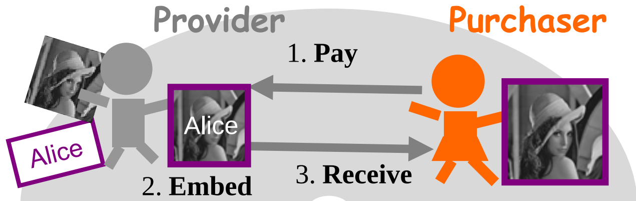
Practical & Secure Content Trading System

A Web-Based Privacy-Secure Content Trading System for Small Content Providers Using Semi-Blind Digital Watermarking

Mitsuo OKADA , Yasuo OKABE, Tetsutaro UEHARA (Kyoto University, Japan)

Conventional Digital Fingerprinting



Summary

1. **Pay** digital cash
2. **Embed** purchaser's ID
3. **Receive** the content

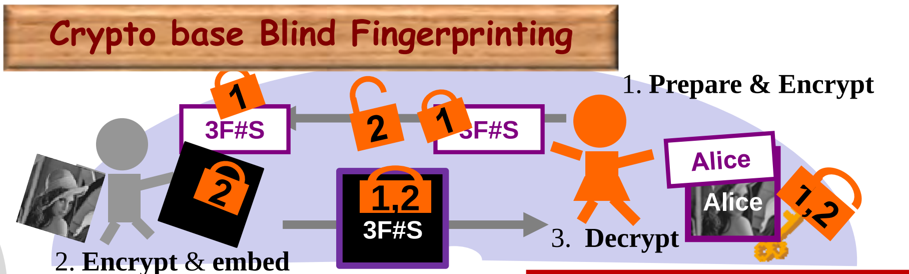
Achievement

Content is protected.

Problem

Privacy isn't **secured.**

Crypto base Blind Fingerprinting



Summary

1. **Prepare** keys and **encrypt** a purchaser's ID.
2. **Encrypt** an image and **embed** the ID into the image.
3. **Decrypt** the embedded image.

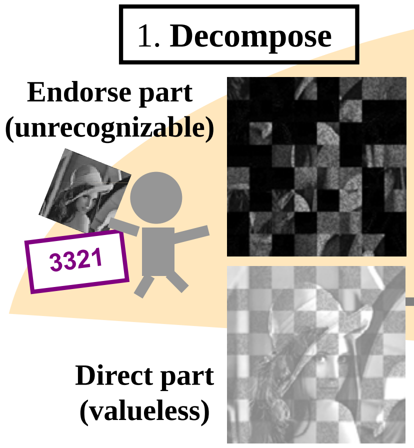
Achievements

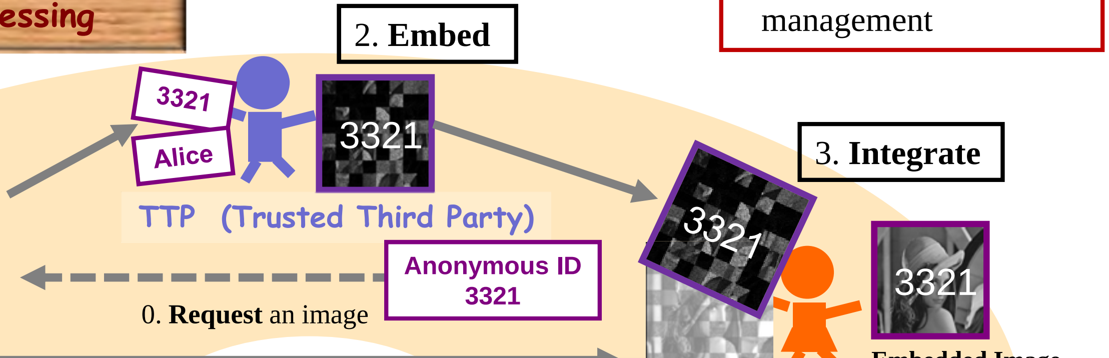
- Content is protected.
- **Privacy** is secured.

Problems (Impractical)

- Heavy computation cost
- Fragile watermark
- Difficulty in key management

Proposed Semi-Blind Fingerprinting Based on Media Processing





Summary

1. **Decompose** an image → a endorse part and a direct part
2. **Embed** an anonymous ID → the endorse part
3. **Integrate** the images → embedded image

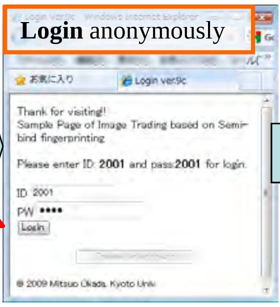
Practical

- **Robust** watermark
- **Feasible** processing cost
- **Easy** to use

Prototype

Start

Login anonymously



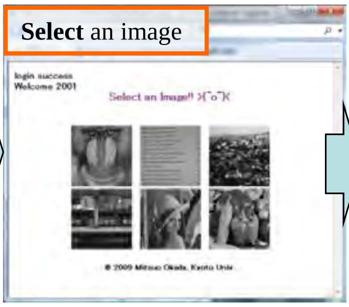
Thank for visiting!
Sample Page of Image Trading based on Semi-bind fingerprinting

Please enter ID 2001 and pass:2001 for login.

ID 2001
PW ••••
Login

© 2009 Mitsuo Okada, Kyoto Univ.

Select an image



login success
Welcome 2001
Select an Image!!)(¯o¯)(

© 2009 Mitsuo Okada, Kyoto Univ.

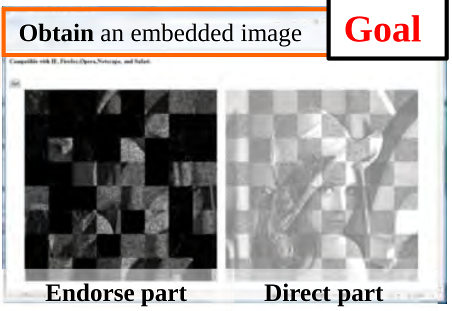
Execute Trading Procedure

Decompose & Embed

Apply Existing Watermark

Obtain an embedded image

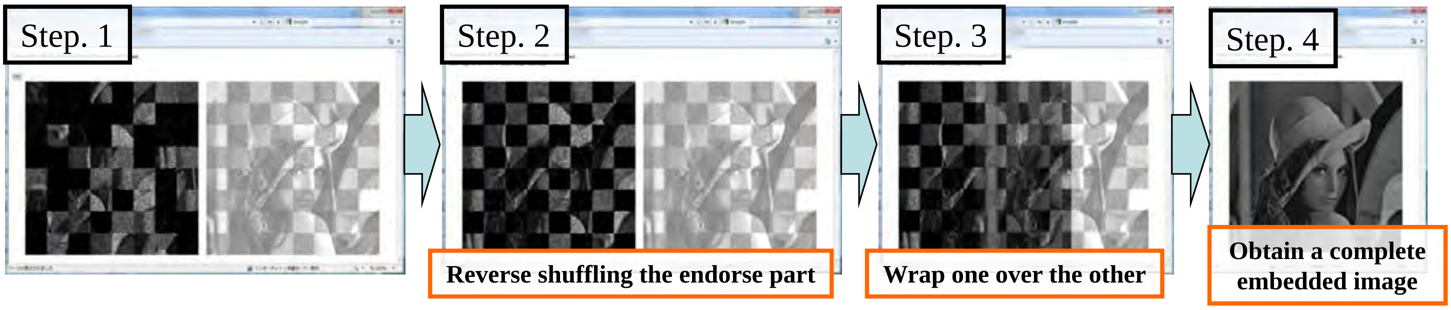
Goal



Endorse part (Unrecognized embedded image)

Direct part (valueless image)

Integration Procedure by the purchaser



Step. 1

Step. 2 — **Reverse shuffling the endorse part**

Step. 3 — **Wrap one over the other**

Step. 4 — **Obtain a complete embedded image**

Practical & Secure Content Trading System

A Web-Based Privacy-Secure Content Trading System for Small Content Providers Using Semi-Blind Digital Watermarking.

IEEE CCNC 2010, Las Vegas.

Mitsuo OKADA, Yasuo OKABE, Tetsutaro UEHARA (Kyoto University, Japan)
Email: mitsuokada@net.ist.i.kyoto-u.ac.jp

Solutions

Our content trading system provides following features.

･**Protecting** purchaser's privacy.

･**Identifying** an illegal party who illegally redistribute a purchased image.

･**Easy** to use. No special tools, skill, nor knowledge is required to use this system.

Digital Fingerprinting

A provider embeds a purchaser's ID into an image using digital watermarking techniques before distributing it to the purchaser. The embedded ID is invisible and unremovable from the image. An illegal user can be identified by extracting the ID from the pirated image when it was found.

Conventional Fingerprinting

Summary

A provider embeds a purchaser's ID before distributing an image.

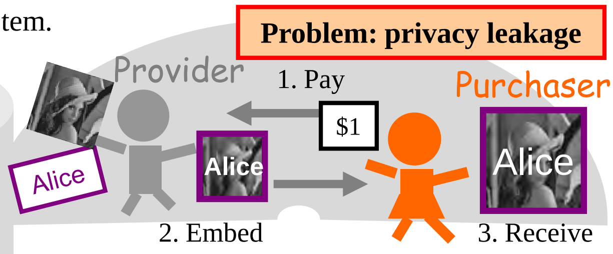
Achievement

Identify an illegal purchaser by extracting the embedded ID from a pirated image.

Problems

•Leakage of purchaser's privacy.

•An illegal party is unable to be identified since both the provider and the purchaser possess the same embedded image.



Problem: privacy leakage

Blind Fingerprinting

Summary

1. A purchaser prepares keys and encrypts the purchaser's ID. Sends them to a provider.
2. The provider encrypts an original image and then embeds the encrypted ID into the image for the purchaser without decryption.
3. The purchaser decrypts an embedded image.

Achievement **(Privacy secure)**

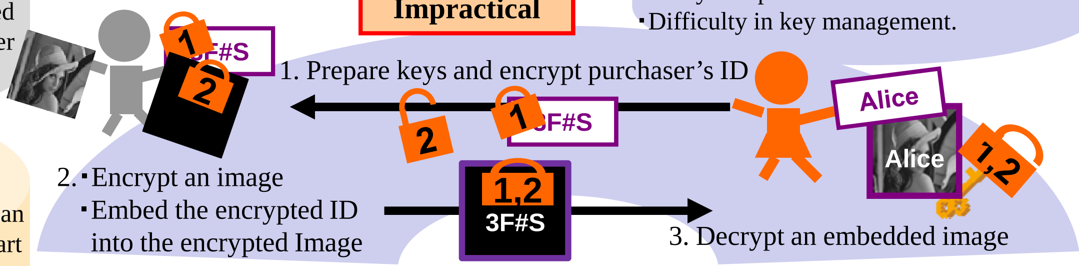
User's information is protected because the ID is encrypted.

Problems **(**Impractical**)**

･Insufficient robustness of watermark.

･heavy computation cost.

･Difficulty in key management.



Impractical

Semi-Blind Fingerprinting

Summary

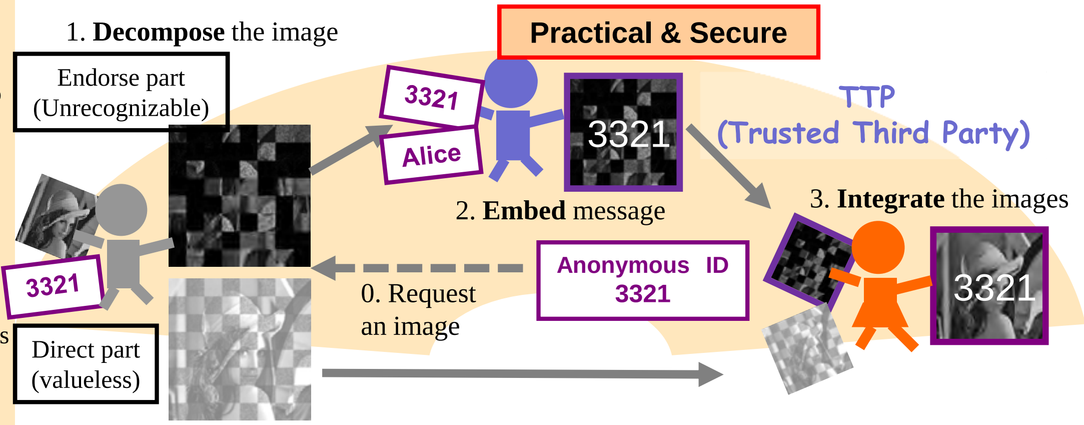
1. A provider **decomposes** an image into an direct part and endorse part. The direct part **(valueless)** is sent to the purchaser and endorse part **(unrecognizable)** is sent to the TTP.
2. The TTP **embeds** an anonymous ID into the endorse part.
3. The purchaser **integrates** two images to generate a complete embedded image.

Achievements

• The illegal party is able to identify since the embedded image can be obtained only by the purchaser.

•Watermark is robust and processing cost is feasible because blinding is non-crypto media processing.

•Privacy is protected. The provider knows the anonymous ID but not the purchaser's name. The TTP knows purchaser's information, but the image is unknown to TTP because of its unrecognizability.



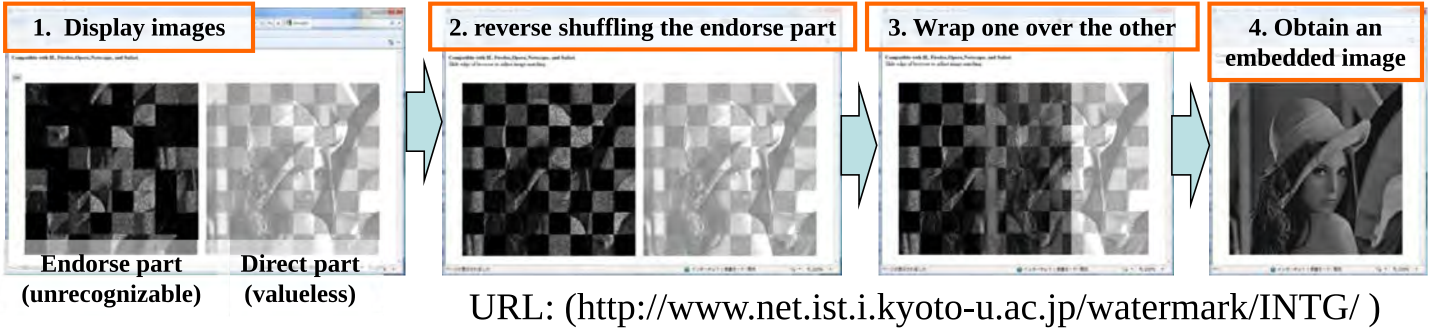
Practical & Secure

･Blind Method
Watermarking⇒Media Process
Blinding ⇒Cryptography

･Semi-Blind Method
Watermarking⇒Media Process
Blinding ⇒Media Process (Non Crypto)

Integration Process

(No special tools, skill, nor knowledge is required); wrapping one of the images over the other



1. Display images

Endorse part (unrecognizable) **Direct part (valueless)**

2. reverse shuffling the endorse part

3. Wrap one over the other

4. Obtain an embedded image

URL: (http://www.net.ist.i.kyoto-u.ac.jp/watermark/INTG/)