安全で実用的なデジタルコンテンツ売買システム

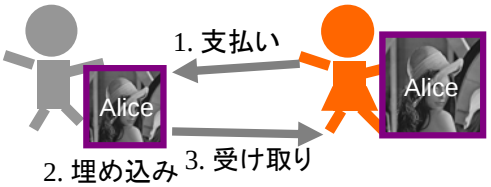
信頼出来ないコンテンツプロバイダに対してもプライバシと コンテンツの保護が可能なインターネットネット画像売買システム

岡田満雄（京都大学　大学院情報学研究科）

従来のデジタルコンテンツ売買

問題点
・プライバシ情報の漏洩
・コンテンツが無防備

コンテンツ保護法



不正コピーコンテンツからIDを抽出し、不正者を特定

問題点
・プライバシ情報が露呈
・不正者の特定が不可能

プライバシセキュア型コンテンツ保護

公開鍵暗号&コンテンツ保護で、プライバシとコンテンツを保護

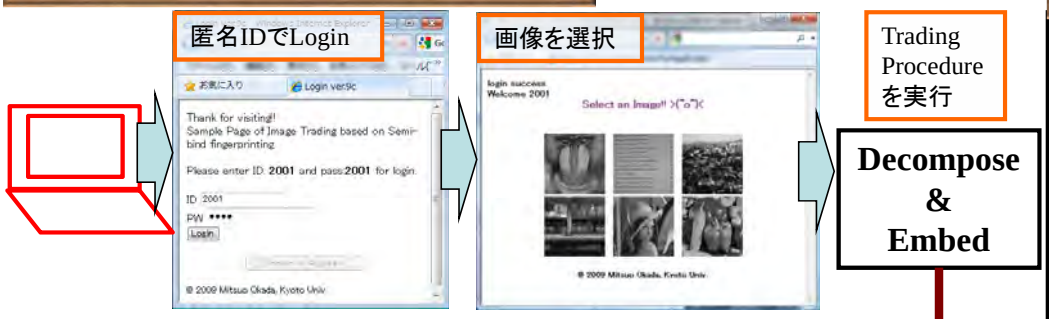
問題点
・非実現的

実用的プライバシセキュア型コンテンツ取引システム

概要
1. 署名用と補完用に**分解**
2. 匿名IDを署名用パーツに**埋め込み**
3.分解された画像を**合体**

解決点
・強い電子透かし
・実用的な計算コスト
・使いやすい

コンテンツトレーディングシステム



実績

受章
IEEE-CCNC2010（米）
→ベストデモンストレーション賞
助成金
・マイクロソフト産学連携研究機構
・京都大学GCOE
国際会議等
多数

ユーザフレンドリー性

デモ有

安全で実用的なコンテンツ取引システム

(信頼出来ないコンテンツプロバイダに対してもプライバシとコンテンツの保護が可能なインターネット画像売買システム)

京都大学ICT イノベーション2010
岡田満雄　京都大学大学院情報学研究科　岡部研究室　博士課程学生
Email: mitsuookada@gmail.com

ゴール

・購入者のプライバシ保護.
・二次配布を行う不正者の特定.
・ユーザフレンドリー.
（誰でも容易に利用可.）

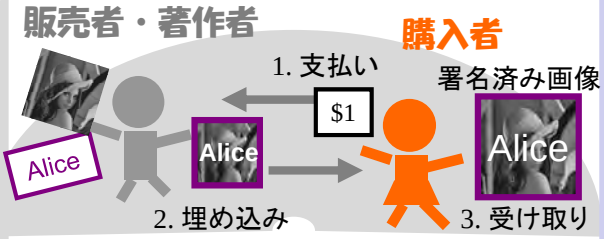
コンテンツ保護

販売者が電子透かし技術を用いて購入者IDをコンテンツに埋め込む. 不正コンテンツが発見された場合, その署名済みコンテンツから埋め込まれたIDを抽出し, 不正者を特定する. IDは識別出来ず取り除くのが困難.

従来型コンテンツ保護

概要
販売者がIDを埋め込み，　配布をする
改善点
海賊版コンテンツからIDを抽出し，不正者を特定
問題点
•購入者のプライバシ情報が漏えい
•販売者と購入者が同じ署名済み画像を保有しているため，どちらが不正者か特定不可能

問題点: プライバシ情報漏えい

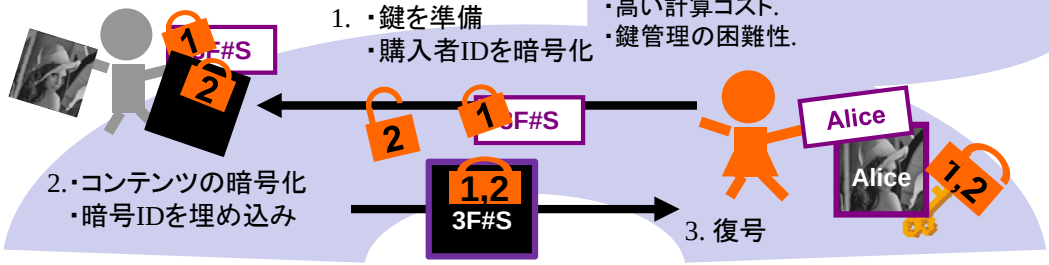


ブラインド型 デジタルフィンガープリント

概要
1. 購入者が公開鍵と秘密鍵を用意. 購入者IDを暗号化し, 公開鍵と暗号IDを販売者に送信
2. 販売者はコンテンツを暗号化. 暗号IDを暗号コンテンツに復号する事なく埋め込む.
3. 購入者は暗号署名済みコンテンツを秘密鍵にて復号.

改善点 (プライバシセキュア)
購入者の情報は暗号化.
問題点(非実用的)
・脆弱な透かし.
・高い計算コスト.
・鍵管理の困難性.

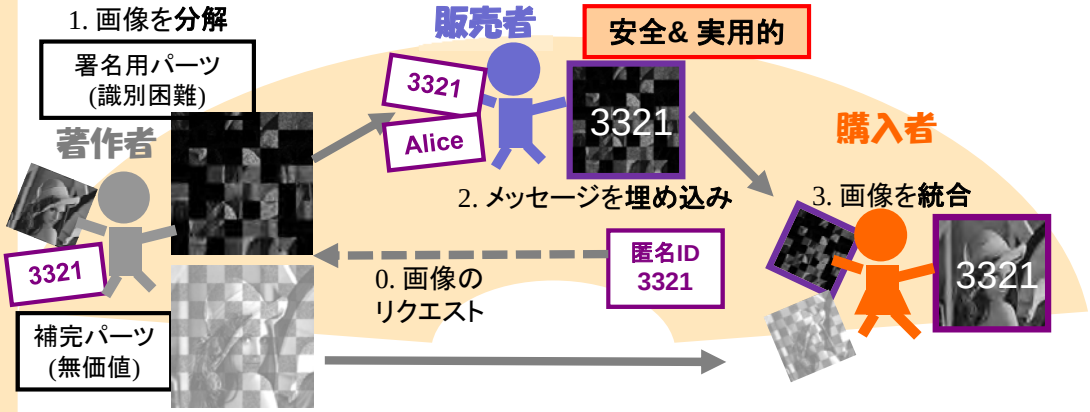
実現困難性



疑似ブラインド型 デジタルフィンガープリント

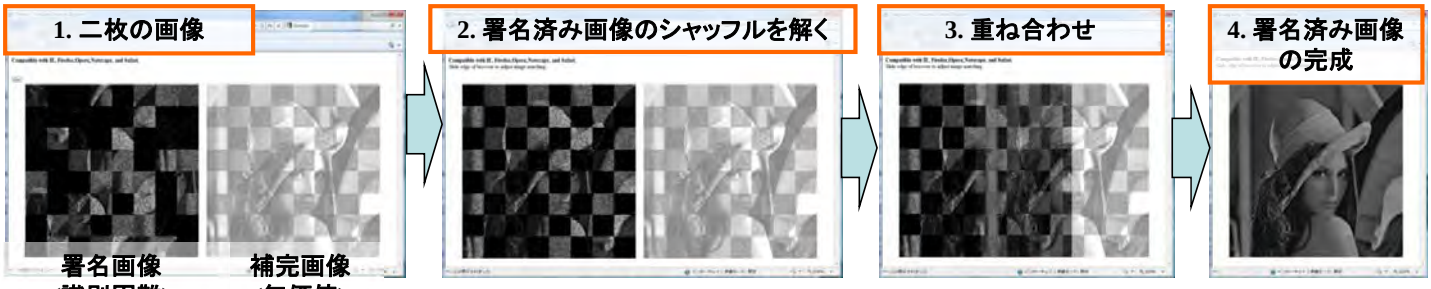
概要
1. 著作者はコンテンツを無価値なパーツと識別不能なパーツに**分解**し, 異なるルートでそれぞれを配信.
2. 販売者はその片辺(識別不能なパーツ)だけに匿名IDを**埋め込む**.
3. 購入者は二枚の画像を**統合**し, 一枚の埋め込み画像を生成 .

改善点
• **否認不能性**: 署名済みコンテンツは購入者しか入手出来ないため、不正コンテンツが発見された場合, 犯人は明らかに購入者と判断できる.
•**頑強性**: 非暗号的メディアプロセスによるブラインド化により頑強な透かしの埋め込みが可能.
•**プライバシの保護**: 著作者は匿名IDを知っているが購入者名は分からない。販売者は購入者情報は知っているが、コンテンツが識別不能なため何を購入しているかは分からない



・ブラインド型	・疑似ブラインド型
透かし処理⇒メディア処理 ブラインド処理⇒暗号	透かし処理⇒メディア処理 ブラインド処理⇒メディア処理 (非暗号型)

統合処理 (特別なツール, スキル, 知識が不要); 重ね合わせ法



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