

# 符号理論・暗号理論

## - No.15 電子透かし技術 -

渡辺 裕

# Coding Theory / Cryptography

## - No.15 Digital Watermarking -

Hiroshi Watanabe

# データハイディング

- 知覚可能形データハイディング
  - 電子透かし
    - 画像や音楽等のデジタルコンテンツに情報を埋め込む
    - 埋め込み情報は著作権関連データ (ex. 作者名, 課金情報, コピー可能回数など)
- 知覚困難形データハイディング
  - ステガノグラフィー
    - 画像や音楽等のデジタルコンテンツに情報を埋め込む
    - 埋め込み情報はコンテンツに無関係であることが多い

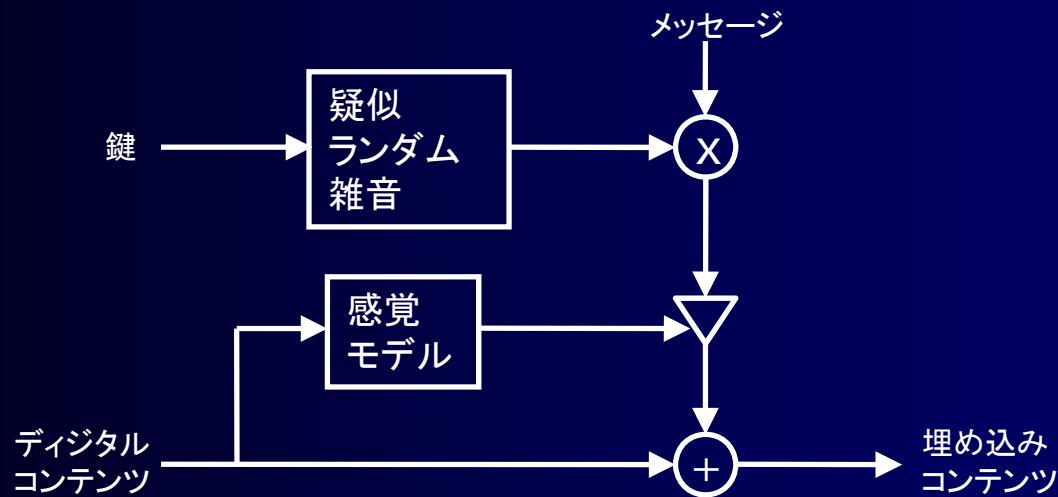
# Data Hiding

- Perceptible data hiding
  - watermarking
    - Embed information to digital content, ex. Image or music
    - Embedded information is IPR data(ex. author, charge, allowed copies, etc)
- Imperceptible data hiding
  - steganography
    - Embed information to digital content, ex. Image or music
    - Mostly embedded information does not relate to content

# アルゴリズム (1)

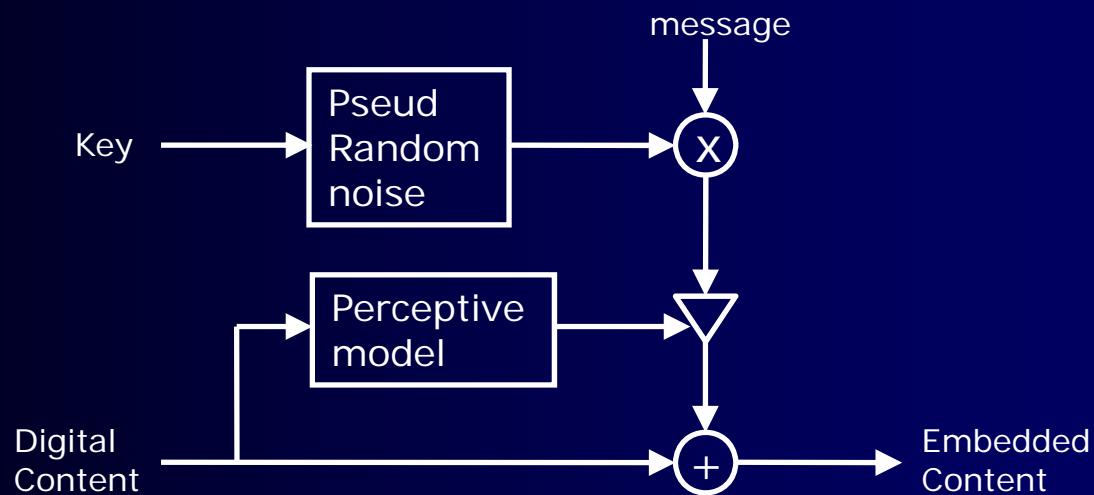
## ■ 情報埋め込み処理

- 複数ビットからなるメッセージを、鍵により生成した疑似ランダムパターンで変調
- デジタルコンテンツに対して感覚モデルを適用し、変調したメッセージの強度を制御して埋め込み



# Algorithm (1)

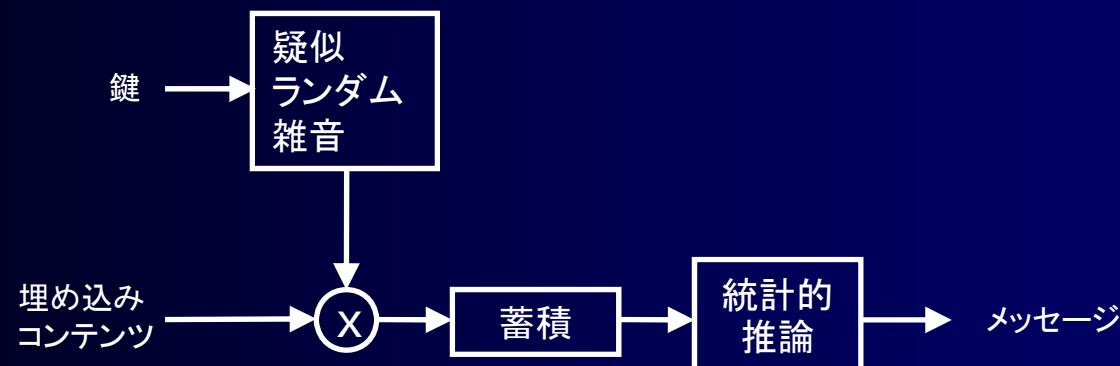
- Information embedding process
  - Modulate message consists of multiple bits by pseud-random pattern generated by a key
  - Apply perceptive model to digital content, control strength of modulated message



# アルゴリズム (2)

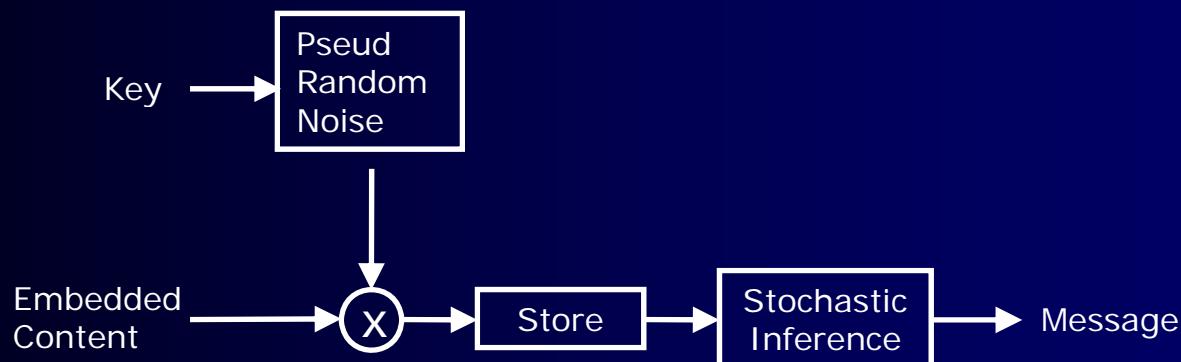
## ■ 情報検出処理

- 埋め込みコンテンツを、鍵により生成した疑似ランダムパターンで変調
- 変調されたコンテンツを蓄積
- 統計的推論によりメッセージを検出



# Algorithm (2)

- Information detection process
  - Modulate embedded content by pseud-random pattern generated by a key
  - Store modulated content
  - Detect message by stochastic inference



# 信頼性

- 電子透かし/ステガノグラフィーの検出時のエラー
  - フォールス・ポジティブ・エラー
    - 埋め込みされていないコンテンツに対して, “埋め込みメッセージあり”と判定する場合
    - ユーザにとってこのエラーが低いことが必要
      - DVD-video:  $10^{13}$ 秒に1回以下, DVD-audio:  $1.5 * 10^{13}$ 秒に1回以下 ( $10^{13}$ 秒 = 300000年)
  - フォールス・ネガティブ・エラー
    - 埋め込みされているコンテンツに対して, “埋め込みメッセージなし”と判定する場合
  - ビット・エラー
    - 埋め込みされているコンテンツから間違ったメッセージを検出してしまうエラー

# Reliability

- Detection error at watermarking/steganography
  - False positive error
    - Judge as “there is an embedded message” to “not embedded content”
    - Low error rate for user is required
      - DVD-video: once at  $10^{13}$  sec, DVD-audio: once at  $1.5 * 10^{13}$  sec ( $10^{13}$  sec = 300000 year)
  - False negative error
    - Judge as “there is not embedded message” to “embedded message”
  - Bit error
    - Wrong message is detected from embedded content

# 耐性 (1)

## ■ ビデオ

- フィルタリングなど一般的にスタジオで使われるビデオ処理
- MPEGの符号化と復号化
- デジタルからアナログへの変換
- ノイズの追加
- 水平方向あるいは垂直方向へのシフト
- 任意倍率での伸縮 (アスペクト比可変)
- 切り取り
- 時系列の順序交換

# Tolerance (1)

## ■ Video

- Video processing generally used at studio such as filtering
- MPEG encoding and decoding
- Digital to analog conversion
- Addition of noise
- Shift in horizontal and vertical direction
- Expansion at arbitrary rate (change aspect ration)
- Cutout
- Change order of time series

# 耐性 (2)

## ■ オーディオ

- 連続する2度のD/A変換・A/D変換
- FMラジオ放送の受信後のA/D変換
- リサンプリングとチャンネル・ミックス
- 音程の変化を伴う時間伸縮, 音程の変化を伴わない時間伸縮
- MP3, AACなどのオーディオ圧縮
- 非線形コンプレッション
- ノイズの追加
- イコライジングなど周波数応答の歪み
- エコー
- バンドパス・フィルター
- ミキシング

# Tolerance (2)

## ■ Audio

- Consecutive two D/A·A/D conversion
- A/D conversion after receiving FM radio program
- Re-sampling and channel mixing
- Time expansion with/without change of tone
- Audio coding such as MP3, AAC
- Non-linear compression
- Addition of noise
- Frequency distortion such as equalizing
- Echo
- Band-pass filtering
- Mixing

# 耐性 (3)

- 耐性のある静止画の電子透かし
  - フィルタリング
  - 圧縮と非圧縮
  - 切り取り
  - 幾何学的変換
    - ローテーション, ズーム, アスペクト比の組合せ
  - レタリング
- 改ざん検出のための静止画電子透かし
  - 画像IDとディジタル署名をJPEG圧縮データへ埋め込み
  - 圧縮状態, 復号画像のどちらからでも検出可能
  - 画像の改ざん位置の検出も可能

# Tolerance (3)

- Tolerant still image watermarking
  - filtering
  - Lossy and lossless
  - Cutout
  - Geometric transform
    - Combination of rotation, zoom, aspect ratio
  - Lettering
- Still image watermarking for detecting falsification
  - Embed picture ID and digital signature to JPEG coded data
  - Detectable both from coded and decoded images
  - Location of falsification can be detected

# 耐性 (4)

- 静止画に対する可視透かし
  - 不正使用に対する抑止効果
  - ロゴマークや著作権を可視状態で埋め込み

# Tolerance (4)

- Visible watermarking to still image
  - Deterrent effect to unauthorized use
  - Embed logo and IPR with visible status

# 埋め込み技術

## ■ 電子透かしの場合

- スペクトル拡散
  - 加法的な改ざんなどに対応できる埋め込み技術
- 量子化レベル制御
  - 頑強ではないが、埋め込み情報量が多い
- 振幅変調
  - 加法的な改ざんに対応、特に空間領域での処理

# Embedded technology

- Watermarking
  - Spread spectrum
    - Embedded technology to additive falsification
  - Control quantization level
    - Less robust, lot of embedded information
  - Amplitude modulation
    - Respond to additive falsification, especially in space domain

# アプリケーション

- ビデオ
  - インターネットでのビデオ配信
- オーディオ
  - インターネットでの音楽配信
  - コマーシャル放送回数のカウント
  - 再生回数のカウント
- 静止画
  - インターネットでの改ざん検出
  - セキュアデジタルカメラ
    - ロスレス電子透かし, 生体認証と電子署名ハッシュ

# Application

- Video
  - Video distribution on the Internet
- Audio
  - Music distribution on the Internet
  - Count numbers of commercial broadcasting
  - Count numbers of playback
- Still image
  - Detection of falsification on the Internet
  - Secure digital camera
    - Lossless watermarking, biometric certification and digital signature hash function

# 可視電子透かしの例

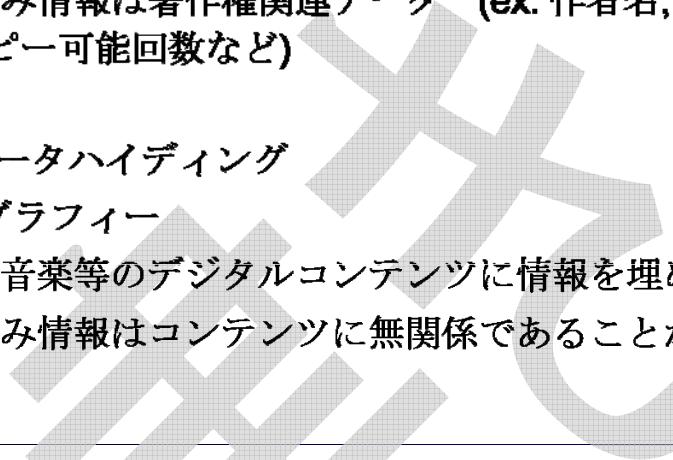
## ■ MS-word

### データハイディング

- 知覚可能形データハイディング
  - 電子透かし
    - 画像や音楽等のデジタルコンテンツに情報を埋め込む
    - 埋め込み情報は著作権関連データ (ex. 作者名, 課金情報, コピー可能回数など)
- 知覚困難形データハイディング
  - ステガノグラフィー
    - 画像や音楽等のデジタルコンテンツに情報を埋め込む
    - 埋め込み情報はコンテンツに無関係であることが多い

# Example of Visible Watermarking

## ■ MS-word



データハイディング

- 知覚可能形データハイディング
  - 電子透かし
    - 画像や音楽等のデジタルコンテンツに情報を埋め込む
    - 埋め込み情報は著作権関連データ (ex. 作者名, 課金情報, コピー可能回数など)
- 知覚困難形データハイディング
  - ステガノグラフィー
    - 画像や音楽等のデジタルコンテンツに情報を埋め込む
    - 埋め込み情報はコンテンツに無関係であることが多い