

村谷 博文
MURATANI Hirofumi

加藤 拓
KATOH Taku

遠藤 直樹
ENDOH Naoki

デジタル化された映画や音楽といったマルチメディアコンテンツの著作権保護が重要な問題となっている。電子透かし技術は、その解決の鍵(かぎ)を与えると期待されている。当社は、従来のスペクトラム拡散法を改良して、埋込み処理や検出・抽出処理の効率化やハードウェアの低コスト化に優れた電子透かし方式を開発した。さらに、この方式は、埋込みにおけるコンテンツの品質劣化を小さく抑える効率的な画像適応を行なっている。また、非可逆圧縮に対する耐性も改良されている。

Finding methods to protect the copyrights of digitized multimedia contents has recently become a serious problem. Watermarking technology is expected to be a key technology providing a solution to this problem.

We have developed a new watermarking method which is based on the spread-spectrum watermarking approach. The advantages of this method are its efficiency in both embedding and detecting/extracting watermarks, and its low hardware cost. Furthermore, this method realizes efficient image adaptation to suppress degradation of the quality of contents induced by embedding. Robustness against lossy compression is also improved.

1 まえがき

デジタル化されたマルチメディアコンテンツはコピーが容易である。映画や音楽などの優れたコンテンツがデジタル化されて流通するには、著作権保護のしくみが必要となる。従来の著作権保護は、記憶媒体や論理フォーマットのくふうによっていたが、最近、コンテンツ自体に電子透かしを埋め込み、セキュリティを高めようとする動きがある。

電子透かし技術は、コンテンツの品質劣化を抑えつつ、さまざまなコンテンツ操作や攻撃による消失・改ざんがない透かし情報を埋め込む必要がある。この課題に対して、スペクトラム拡散による電子透かし方式が有望視されている⁽¹⁾⁽²⁾。

この方式はコンテンツの周波数領域で透かし情報の埋込みや検出を行うため、周波数変換の処理コストが大きい。当社は、スペクトラム拡散法の特長を残しつつ、周波数変換の計算コストを軽減する電子透かし方式を考案した。動画像や音楽に対する実時間における電子透かしの埋込み・検出を容易にし、ハードウェアコストを削減する効果が期待される。

2 電子透かしとは

電子透かしとは、デジタル化された静止画、動画、音楽といったマルチメディアコンテンツの中に、透かし情報を埋め込む技術である(図1)。コンテンツに小さな変化を

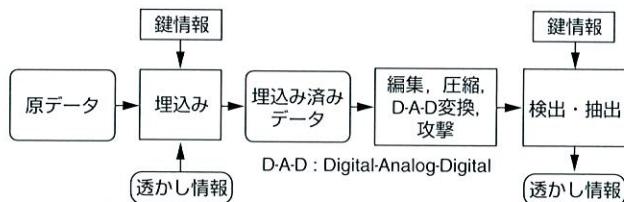


図1. 電子透かしのスキーム 埋込みと抽出・検出の二つのプロセスがある。電子透かしが埋め込まれているか否かの判定処理は検出、埋め込まれた透かし情報の復元処理は抽出と呼ばれる。
Digital watermarking scheme

与えて透かし情報を表現する処理を“埋込み”と呼ぶ。

一方、埋込み済みコンテンツから透かし情報を復元する処理を“抽出”と呼ぶ。また、透かし情報が埋め込まれているか否かを判定する処理を“検出”と呼ぶ。検出・抽出では、埋込み時に与えた擬似乱数列のシード^(注1)などのパラメータを鍵情報として必要とする。

電子透かしの利用方法は、さまざま提案されているが、以下が主なものである。

- (1) 著作権者名やコンテンツ識別番号などの著作権情報を埋め込み、二次利用を容易にしたり、著作権侵害を発見したりする(図2(a), (b))。
- (2) 利用者名や購入者名などの利用者情報を埋め込み、海賊行為者の特定や海賊行為の抑止に利用する(図2(c))。

(注1) 擬似乱数を生成する回路(関数)が毎回同じ系列を生成するがないように初期値として与える数。

(3) 利用・コピー制御情報を埋め込み、再生・コピー機能をもつ機器での不正な利用やコピーを防止する(図2(d))。

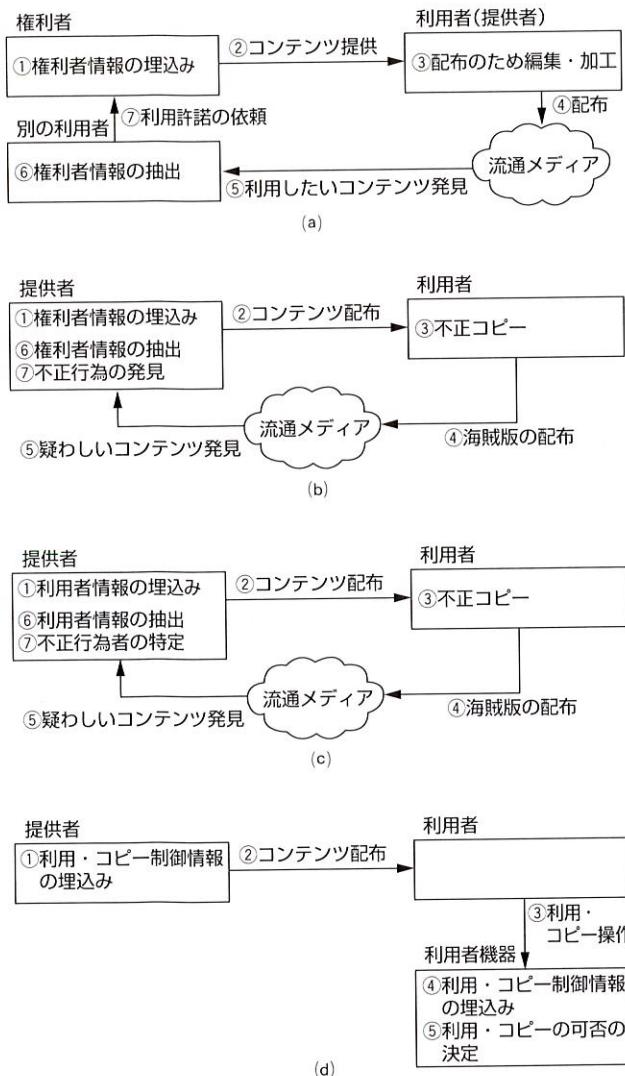


図2. 電子透かしの利用形態 電子透かしには、(a)のようにコンテンツの流通を促進する光の側面と、(b)から(d)のように著作権侵害を抑止・防止する陰の側面がある。

Applications of digital watermarking

上記のような利用方法を前提にして、電子透かしに対する要件には、以下のようなものがある。

- (1) 電子透かしは、分離が容易なフォーマット上のヘッダ部や特定フィールドではなく、コンテンツ自身に埋め込まれる。
- (2) 埋込みによって生ずるコンテンツの品質劣化が知覚されない。
- (3) 編集・加工や非可逆圧縮などコンテンツに対して通常に施される操作や意図的な攻撃を行なっても、コン

テンツに対して著しい品質劣化を与えることなく、透かし情報を消失させたり改ざんしたりできない。

- (4) 同じコンテンツに異なる利用者情報を埋め込んだ二つ以上のコンテンツを用いて、利用者情報を消失させたり改ざんしたりすることが困難である。
- (5) 埋込みや抽出・検出処理が効率的に行える。
- (6) 利用に必要なサイズの透かし情報を埋め込むことができる。

上の(2)と(3)の要件の間には、トレードオフが存在する。例えば、非可逆圧縮やノイズ付加を行なっても透かし情報を消失しないためには、透かし情報を強く埋め込めばよいが、それはコンテンツの品質劣化の原因となる。スペクトラム拡散法による電子透かし方式は、この問題に対する解決を与えている。

3 スペクトラム拡散法

スペクトラム拡散は、本来、通信において妨害信号の干渉を防ぐため、送信したい信号を非常に広い帯域に拡散変調する考え方である。スペクトラム拡散による電子透かし方式では、拡散された電子透かし信号がコンテンツに埋め込まれる。加工や非可逆圧縮や攻撃に起因するノイズ信号がコンテンツに加わっても、逆拡散によって電子透かしを復元することができる(図3)。また、電子透かしはコンテンツ全体に拡散されるので、コンテンツの一部の切出しや周波数フィルタリングに対しても、電子透かしを復元できる。スペクトラム拡散は、広帯域のノイズ付加に対して効果はないが、かりに、電子透かしを消失させることができたとしても、コンテンツの品質劣化が著しい。

スペクトラム拡散による電子透かし方式には、電子透かしの標本値領域において、 ± 1 に値をとるPN系列(Pseudo-

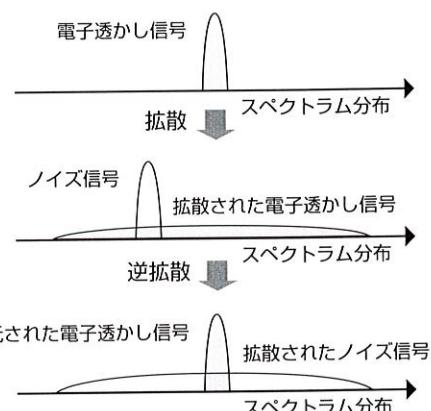


図3. スペクトラム分布の変化 電子透かし信号は拡散と逆拡散で同じ擬似乱数列が乗積されて元にもどるが、ノイズ信号は1回しか乗積されないので拡散される。

Changes of spectrum distribution

random Number sequence) による拡散を行う直接拡散法⁽¹⁾と、コンテンツの周波数領域において、正規分布に従う実乱数列を電子透かしとして埋め込む摂動法⁽²⁾の二通りの異なる方式が提案されている(図4)。

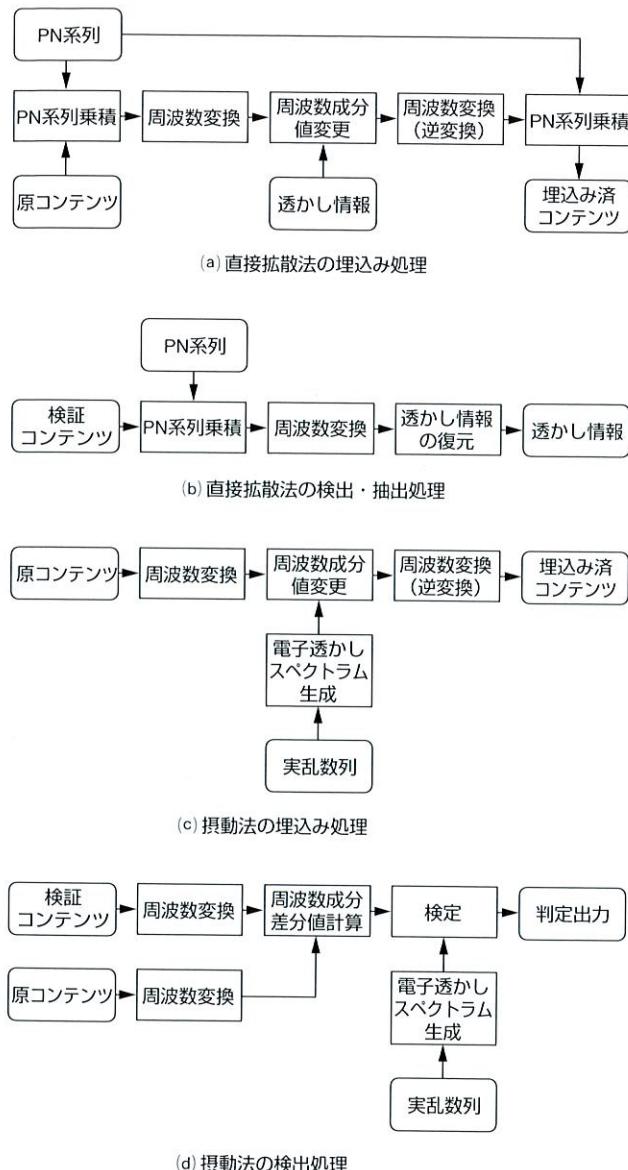


図4. 直接拡散法と摂動法　直接拡散法は標本値領域における直接拡散のあと周波数変換を行う。摂動法は周波数変換により周波数領域に移ってから拡散を行う。

Spread-spectrum watermarking approaches in spatial domain and frequency domain

スペクトラム拡散法は、埋込みと検出・抽出の両方で周波数変換を行う。周波数変換は比較的処理の負荷が大きい。特に動画に対して実時間処理を行うためには、ハードウェア化が必須(す)である。さらに、JPEG (Joint Photographic Experts Group) や MPEG (Moving Picture Experts

Group) 圧縮の離散コサイン変換は8×8画素の小さな画像ブロックに対して適用されたのに対し、スペクトラム拡散法では、128×128画素から512×512画素の大きな画像ブロックに対して適用されるため、高速化のためのコストが大きい。この周波数変換のコストを軽減するためのくふうを行なったので、以下にそれを紹介する。

4 埋込みと検出・抽出の効率化

スペクトラム拡散法は、次の二つの理由から周波数変換を必要とする。

- (1) 電子透かしの埋込みや検出・抽出を周波数領域で行う。
- (2) 電子透かしの埋込み強度をコンテンツの性質に応じて変化させる(画像の場合、画像適応)。

当社は、周波数変換の処理コストを軽減するため、直接拡散法を採用し、さらに、埋込み対象となる周波数成分は少数とした。そのうえで、埋込み処理において、周波数変換とその逆変換は行わずに、周波数成分値の変分から標本値の変分を直接計算する。また、検出・抽出処理においても、周波数変換を行わずに、埋込み対象となった周波数成分値だけを計算する。計算すべき周波数成分の数が小さい場合には、周波数変換を行うより高速にその値を求めることができる。

この方式では、画像全体を一つのブロックとして埋込みや検出・抽出を行う場合でも、効率良い処理が可能である。また、ハードウェア化のコストも小さくて済む。例えば、コンテンツの品質劣化を極力抑えて利用制御情報を埋め込む場合、大きなブロックサイズを選択することが好ましい。そのような場合、この方式が有効である。

5 画像適応による信頼性向上

一般に、画像適応を行うことによって、品質劣化を増すことなく、電子透かしの検出・抽出の信頼性を向上させることができる。この方式では、画像ブロックごとにその性質を反映した埋込み強度を用いることにより画像適応を行う。

電子透かし検出の信頼性に関する指標に偽陽性率(false positive ratio)がある。これは、検出において電子透かしが埋め込まれていないコンテンツに対して、電子透かしが埋め込まれていると誤って判定する確率である。

ある周波数成分値がある閾(いき)値Tを超えた場合には電子透かしが埋め込まれている、そうでない場合には埋め込まれないと判定する検出アルゴリズムを例に説明する。

直接拡散法では、標本値にPN系列を乗積するため、周波数成分値の頻度分布はほとんどガウス分布となる(図5)。

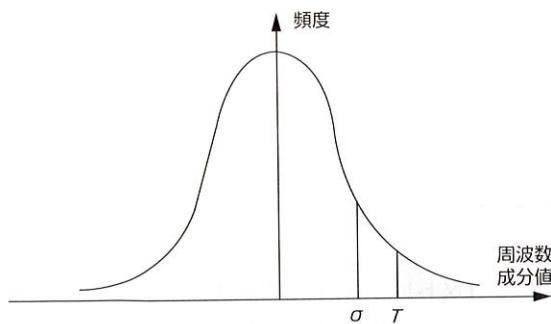


図5. 拡散画像の周波数成分値分布 拡散画像の周波数成分値はガウス分布に近い分布になる。

Frequency coefficient distribution of spread images

埋込み強度が一定では、偽陽性率は標準偏差 σ が小さなブロックでは偽陽性率は小さく、 σ が大きなブロックでは偽陽性率は大きくなってしまう。そこで、 σ が小さなブロックでは埋込み強度を小さく、 σ が大きなブロックでは埋込み強度を大きくするような画像適応を行う。

σ は周波数変換なしに計算できる。周波数成分値の分散は、周波数変換の直交性によって式変形すると、拡散前の標本値の二乗平均に等しいことがわかる。この量は、周波数変換なしに効率的に計算できる。

6 非可逆圧縮耐性の向上

摂動法と比較して、直接拡散法の最大の欠点は、非可逆圧縮に対する耐性が劣っていることである。摂動法は、周波数領域中における埋込み対象となる周波数成分を低中間周波数と設定することで、埋め込まれる電子透かしの周波数を直接制御することができる。したがって、非可逆圧縮の圧縮の程度に応じて、透かし情報が消失しないよう制御が行えた。ところが、直接拡散法では、埋込み対象の周波数成分をどこに設定しても、PN系列による変調のため電子透かしのエネルギーの多くは高周波成分に配分されてしまう。

この問題に対して、画像ブロックのサイズを大きくして拡散率を高めることにより透かし情報の消失を防ぐアプローチがある⁽³⁾。しかし、埋め込める透かし情報のサイズが小さかった。この方式では、拡散時に個々の乱数値をそれ

ぞれ一つの標本値に対応させるのではなく、 2×2 画素といった複数の標本値を含むブロックに対応させ、その内の標本値すべてに同一の乱数値を乗積する方法を採用することで、直接拡散法で電子透かしの周波数を直接制御する。これにより、実質的に埋め込まれる電子透かしの周波数を制御することができ、摂動法に匹敵する圧縮耐性を実現できる。

7 あとがき

マルチメディア情報の著作権保護への応用が期待されている電子透かし技術を紹介し、当社が開発した埋込みや検出・抽出を効率的に行える電子透かし方式について述べた。この方式は、特に、動画や音声などリアルタイムでの電子透かしの検出・抽出が必要な場合や利用者情報を埋め込む利用形態への応用が期待される。

文 献

- (1) 大西淳児、他。“PN系列による画像への透かし署名法”。1997年暗号と情報セキュリティ・シンポジウム。福岡、1997-01、電子情報通信学会情報セキュリティ研究専門委員会、1997、26B。
- (2) Cox, I., et al. “A Secure, Robust Watermark for Multimedia”. Information Hiding. Ross Anderson. Cambridge, 1996-05. Springer-Verlag, 1996, p.185-205.
- (3) 村谷博文、他。“直接拡散による電子透かしの耐性評価”。1999年暗号と情報セキュリティシンポジウム。神戸、1999-02、電子情報通信学会情報セキュリティ研究専門委員会、1999、p.503-508。



村谷 博文 MURATANI Hirofumi, D.Sci.

研究開発センター コンピュータ・ネットワークラボラトリーア研究主務、理博。セキュリティシステムの研究・開発に従事。情報処理学会、IEEE会員。
Computer & Network Systems Lab.



加藤 拓 KATOH Taku, D.Eng.

情報・社会システム社 SI技術開発センター SI技術担当、工博。情報セキュリティ技術および応用システムの研究・開発に従事。電子情報通信学会会員。
System Integration Technology Center



遠藤 直樹 ENDOH Naoki

情報・社会システム社 SI技術開発センター 戰略企画担当主幹。情報セキュリティ技術および同技術応用システム技術の研究・開発に従事。電子情報通信学会、日本セキュリティマネジメント学会会員。
System Integration Technology Center