デジタルメディアへのデータハイディング

1N－12

森本典繁　清水周一　沼尾雅之
日本アイ・ビー・エム（株）東京基礎研究所

1．はじめに

近年のデジタル・メディアの増加に伴い、ネットワークを流通するデジタル・コンテンツのセキュリティーや知的所有権の保護が重要な課題となっている。コンテンツの通信路上の保護は、従来より暗号化による保護が用いられているが、正規に入手し、復号化されたデーターや、暗号化されていない著作物の違法な複製や再配布の阻止や検出を行う手段は現在のところないため、これらの違法行為は事実上野放し状態にある。データー・ハイディングは、デジタル・コンテンツと不可分でかつ非可視なマーキング（または付加的な情報の埋め込み）を施すことができる技術で、流通するコンテンツに著作権者名や出版者名、製品番号などの情報を埋め込めば、違法コピーの検出やその流通経路の特定が可能になる。本稿では、データー・ハイディング技術の特徴、技術課題および応用例について説明する。

2．データー・ハイディングとは

データー・ハイディングとは、画像や音声のデジタル・コンテンツに、利用者に検知されない形で付加情報を埋めこむ技術の総称である[1]。本技術のもうひとつの特徴としては、付加情報が媒体であるコンテンツと不可分であることがあげられる。情報を追加するのではなく、媒体のデーターを修正して所定の情報を表現させるため、一般的な編集や加工によるフォーマットの変更やヘッダ情報の喪失によっても埋め込まれた情報が失われずに残る利点がある。この特徴を利用して、所有者情報や配布履歴等の情報を流通するコンテンツに埋めこめば、著作権の保護に役立てることができる。[1, 2]

技術的課題

データー・ハイディングでは、コンテンツを構成する要素に直接操作を施すことにより、コンテンツと埋めこむ情報を不可分にしているが、この操作によって生じるコンテンツの劣化（画質や音質）には、利用形態やユーザの要求により制限が課せられる。すなわち、情報の埋め込みに使用できるデータ領域の大きさが制限される。一方、著作権の保護などに応用する場合、悪意を持つ利用者による埋め込み情報の除去や加工に対してある程度の耐性をもつ必要があるが、この耐性は埋めこむ情報の冗長度によって左右される。この様に、コンテンツの質、埋めこむ情報の量、及び加工に対する耐性はお互いにトレード・オフの関係にあり、この妥協点をいかに引き上げるかが本技術の課題となる。さらに、著作権の保護の観点から、鍵の生成や改ざんの防止等も実用化への課題となる。利用形態により、各要求項目の優先度や要求レベルが大きく変わるが、以下に、我々の考えるマーキング技術の要求事項を整理した。

基本要求事項

1. データーの埋め込みに起因する画質や音質等の劣化は、利用者が検知できないレベルであること。
2. 埋めこまれた情報は、一般的なコンテンツの編集や圧縮に対しても安定して抽出できること。
3. 改ざん防止の為、情報の埋め込みと抽出には異なる鍵を用いる（公開鍵方式の暗号技術を応用）。
4. 利用者側の環境下で情報の検出・抽出をする為、検出・抽出のオーバーヘッドは十分小さいこと。
5. 正規に入手した複数のコピーを用いて埋め込み情報を不法に取り出そうとする行為に対する耐性があること。
6. 埋め込める情報の長さは、個体識別の観点から最低32-64ビット以上で、かつ可変であること。
7. 制限なく、幅広く媒体のサイズやフォーマットの種類に対応できること。

3．データー・ハイディング技術の応用

本技術は、デジタル・コンテンツに、付加情報を伝達できる擬似的な副チャネルを設ける技術であり、埋めこめる情報は、識別番号など数値や記号に限らず、会社のロゴなどのイメージ情報も含まれる。その用途は、キャプションや編集履歴の記録、多様な異なる形式のデーターへの統一したタグ情報の付加など、多岐にわたっている。本項では、特に著作権の保護に関する応用案について述べる。

個人認証・デジタル署名（所有者情報の埋め込み）

情報の授受において、情報の出所や真贋の確認が必要な場合がある。一般的に、公開鍵方式の暗号技術を用いることにより実現可能であるが、データー・ハイディング技術と組み合わせることにより、流通するコンテンツ自身を、暗号コードの伝達媒体として利用でき、暗号とコンテンツを不可分にすること

Data Hiding Techniques for Copyright Protection
Norishige MORIMOTO, Shuichi SHIMIZU, Masayuki NUMAO.
IBM Japan Ltd., Tokyo Research Laboratory.

ができる。この場合、コンテンツの変更を敏感に検知できることと、第三者による改ざんが容易にできないことが条件となる。

デジタル透かし（送り手情報の埋め込み）

配布したコンテンツの所有権を主張したり、違法コピーの存在を検知する為のマーキングをデジタル透かし(digital watermark)と呼ぶ。埋めこむ情報は、所有者の識別番号やロゴなどのイメージが対象となるが、コンテンツにＩＤを埋めこみ、受信側で自動的に検出することにより、コンテンツの配布数量の記録や違法コピーの検出を行うこともできる。この場合、埋めこむ情報量よりもコンテンツの編集や圧縮等の加工に対しても耐性が重要となる。また、利用者側の環境下で埋め込んだ情報の検出を行うためには、検出操作の計算量の負荷が軽くなければならない。

デジタル指紋（受取り手情報の埋め込み）

コンテンツの送信時に、受取り手のＩＤ情報（名前、クレジットカード番号等）を、コンテンツに埋めこんで送付する利用形態をデジタル指紋（digital fingerprint）と呼ぶ。コンテンツの受け渡しが行われる度に、受取り手の情報を埋めこんでおけば、違法コピーが出まわった場合、そのコピーから流出元を割り出すことができる。また、複数回の受け渡しが行われた場合に、受け渡しの都度に埋め込まれる受け取り手情報から、配布経路を追跡することも可能である。サービスとして合法的に情報を再配布する場合（大学、図書館や企業）、違法行為の責任回避の観点からも、二次利用者のＩＤ情報を埋め込むインセンティブがある。

４．技術の概要

静止画像におけるデーター・ハイディング

一般的に、データー・ハイディングの方法は下記の様に分類できる。

- 統計的な性質を利用する方法
- 周波数空間を利用する方法
- 局部的な性質を利用する方法

統計的な性質を利用する場合、画像の加工により急激に検出精度が下がることがないが、空間的な冗長性に頼るため埋め込める情報量が極端に少ないという欠点がある[1]。周波数空間を利用する方法は、特定の周波数成分除去フィルターや、DCTを用いた圧縮アルゴリズムに対して耐性があるが、一般的に、埋め込んだ情報の抽出にかかる負荷が大きく埋め込める情報量も少ない[3]。我々が開発した方法は、三番目の画像の局部的な特徴を利用している。埋め込む情報は、二値のビット列に変換された後、それぞれのビット値が、画像内の指定された画素（群）に埋め込まれる。主な技術要素は、埋め込み操作の対象となる画素（群）の選択アルゴリズム[4]と、画素値の操作方法[5]の二つである。前者は、選択された画素（群）が画像内に一様に分布し、かつ埋め込みと抽出の鍵を非対称にできるため、公開鍵方式でのデジタル署名が実現できる。後者は、ビット値を、選択された画素（群）に局部的な画質の特徴として埋め込む方法で、情報の抽出が自動で、かつ画質の劣化が小さいため、多くの情報を埋め込むことが可能である。さらに、対象となる画素（群）の範囲を広げることにより、ＪＰＥＧの画像圧縮やその他の加工に対して高い耐性を持たせることができる。

音声におけるデーター・ハイディング

音声情報も、画像同様、上記のアイデアの応用が可能であるが、音声では、再利用に際し、部分の切り出しが頻繁に行われる為、短いセグメントからでもデーターが抽出できる様に、分散度を高めることと、埋め込まれたデーターの開始／終了位置の検出精度が鍵となる。音声へのデーター・ハイディングの手法としては、下記の方法がある。[1]

- 拡散周波数スペクトラムを用いる方法
- 音声の位相成分を用いる方法
- 音声のエコーを応用する方法
- 音声の局部的な類似性を利用する方法

５．今後の発展

著作権保護への利用を考えた場合、本技術は違法コピーの検出によって違法行為に対する歯止めにするもので、この技術だけで直接的なコピー防止を行うことはできない。今後は、暗号技術と、データー・ハイディング技術を組み合わせ、コンテンツの製作から利用までの各場面を想定した、包括的な著作権保護のシステムを構築する必要がある。

参考文献

1. W. Bender et al.: "Data Hiding Techniques", In Proc. SPIE vol.2020-40. Feb. 1995.
2. Jian Zhao, et al.: "Embedding robust labels into images for copyright protection", In Proc. of the Int. Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, Aug. 1995.
3. Ingemar J. Cox, et al.: "Secure Spread Spectrum Watermarking for Multimedia", NEC Research Institute, Technical Report 95-10, 1995.
4. 沼尾他：”データハイディングによる署名技術”、In Proc. of IPSJ 53th annual conference, 1996.
5. 清水他：”ピクセルブロックによる静止画像データハイディング”、In Proc. of IPSJ 53th annual conference, 1996.