4K－4

多数フレーム解析に対するデータハイディングのセキュリティ

清水 周一
日本アイ・ビー・エム株式会社 東京基礎研究所

1 はじめに

動画や音声などのデジタルコンテンツに対して，IDやコメント，署名などの付加情報を，不可視および不可聴の状態で埋め込んで隠すデータハイディング技術は，所有者証明（Watermarking），追跡（Fingerprinting），再生録画機器の制御，改竄の検出や認証，注釈の添付など，その用途は広く，重要なソリューションコアとして期待されている。

データハイディングの要件としては，（1）品質の保存：コンテンツの価値を下げないために，埋め込み操作の前後で品質をほとんど劣化させないこと，（2）耐性：拡大縮小や切り取りなど一般的な編集作業や，損失のある圧縮処理などを施した後でも埋め込んだ情報（マーク）が抽出できること [3]，（3）抽出の信頼性：マークの有無を誤ることなく高い精度で判定できること，そして，（4）セキュリティ：マークを不正に除去したり改竄したりできないようにすること，などがある．例えば，動画データでの複製許可フラグとして利用する場合には，動画コンテンツの品質を落さないことはもちろん，耐性の条件としては，MPEG2 圧縮に加えて，NTSC などアナログ信号に変換された後でもフラグ検出を行えること，また，複製の制御信号の入っていない動画データからも複製禁止のフラグを誤って抽出する（false positive）ことのない，高い抽出判定の信頼性を実現すること，そして，複製禁止フラグを不正に除去できないようにすること，などの条件が必要である．

本稿では，上記4つの要件のうちセキュリティについて，動画像データに起こる問題点を指摘し，その解消法について説明する．

2 セキュリティ：マークの不正除去

セキュリティの観点から見ると，埋め込んだ情報には，(i) 他の情報への改竄や (ii) 無資格者による不正な読み出し，(iii) 埋め込み情報の消失といった危険が伴う．改竄を防ぐには，埋め込みと抽出アルゴリズムとを非対称にして，埋め込み操作を秘密にすれば良い [2]．不正読み出しを防ぐには，抽出アルゴリズム，あるいは，抽出鍵を秘密にすればよい．しかし，埋め込み情報の消去は，埋め込みおよび抽出のアルゴリズムが不明でも，オリジナルのデータからの差分を破壊することができれば，容易に抽出処理を妨害し埋め込み情報を消失させることができる．埋め込み情報が，例えば，複製禁止のフラグであったとしたら，これは重大な問題である．

同一のコンテンツに対し，マークを変えて埋め込み処理を施したものをいくつか収集し，それらのデータの平均を取ることによって新たなコンテンツを作成するという共謀攻撃（collusion）は，データの品質を損なうことなく，埋め込み情報を破壊するための効果的な手段である．この共謀攻撃が成功するのは，以下に示すように，1種類のコンテンツに対して複数種類のマーキングを施した結果，平均化操作がマークのみを破壊したからである．

$$1/N \cdot \sum_i^N (C + M_i) = C + 1/N \cdot \sum_i^N M_i \to C$$

ここで，C はオリジナルのコンテンツ，M_i は i 番目のマーク，N は平均を取ったコンテンツの数である．

ところで，動画像の各フレームに複製禁止のフラグを埋め込むといった用途を考えると，これは，上記の例とは逆で，複数種類のコンテンツ（フレーム）に対する1種類のマーキングである．したがって，共謀攻撃での平均化操作はフレームを破壊するので目的を果たさないように思えるが，オリジナルのフレームを十分に相殺する数だけ足し合わせると，代わりに，1種類のマークを浮かび上がらせることになる．そのマークは，オリジナルからの差分に他ならない．

$$1/N \cdot \sum_i^N (C_i + M) = M + 1/N \cdot \sum_i^N C_i \to M$$

したがって，各フレームから，このマークを差し引けば，動画像フレームの品質を損なうことなく，埋め込んだ複製禁止のフラグは消失する．

3 ランダム性の導入

前節での動画像の問題を回避するためには，マーク M を固定ではなく，フレームに応じて変化させれば (M_i) 良いが，しかしながら，マークの変化とフラグ検出器のオペレータとを自動で同期させることは一般に困難なので，同期の不要なマークの抽出処理が必要となる．

Datahiding security to statistical analysis on multiple frames
Shuichi SHIMIZU
IBM Japan Ltd., Tokyo Research Laboratory

以下では，同期の不要なオペレータとマークの組合せについて説明し，さらに，マークにランダム性を持たせることにより，前節の問題を回避する方法を示す．

3.1 検出オペレータとマークの直交性

オリジナルの画像データIと埋め込み後の画像データI'との差分をΔとしたとき，オリジナル画像を必要としないマーク抽出は，以下のように表現できる．ここで，O_MはマークMの検出オペレータである．

$$O_M(I') = O_M(I+\Delta) \approx O_M(\Delta)$$

ΔがMに一致する埋め込み方法はもちろん，ΔがIに依存して変化するような埋め込みの場合でも，$O_M(\Delta) \approx O_M(M)$であれば，マーク$M$の抽出は成功する．周波数空間での変更による埋め込み手法[1, 3]や，実空間でのコヒーレントな変更による埋め込み方法もこの分類にあたる．

さて，互いに異なる２種類のマークについて，それぞれを検出するための２つのオペレータが，互いのマークに対しては検出反応を示さないとき，その２つのマークを互いに直交であると呼ぶことにする．互いに直交するマークは，例えば，画像の空間周波数に対して，互いに異なる周波数成分に反応するように構成するなどして実現できる．Tはマークの有無を判定する閾値である．

$$\begin{aligned} O_{M_i}(M_j) &> T \quad (i=j) \\ &< T \quad (i \neq j) \end{aligned}$$

何種類かの，互いに直交するマークのうち１つがフレームに埋め込まれていて，しかし，どのマークが使われたか不明であるときには，すべてのマークに対応するオペレータをそれぞれ適用し，その中で最大に反応したものを採用することにより，マークの有無判定および検出ができる．このように，オペレータとマークの直交性を利用すれば，検出処理のコストはたかだかオペレータの種類に線形に増えるだけで，マークとオペレータの対を一致させるための同期が不要となる．

$$\begin{aligned} \max(O_{M_1}(I'), \ldots, O_{M_m}(I')) &> T \quad \text{(marked)} \\ &< T \quad \text{(nomark)} \end{aligned}$$

3.2 マークのランダム選択

互いに直交するマークをm個用意し，それをランダムに選んでフレームに埋め込んだとき，フレームの平均化操作は，以下に示すようにm個のマークの平均値をもたらす．

$$\begin{aligned} 1/N \cdot \textstyle\sum_i^N (C_i + M_{k_i}) &\rightarrow 1/N \cdot \textstyle\sum_i^N M_{k_i} \\ &\rightarrow 1/m \cdot \textstyle\sum_j^m M_j \end{aligned}$$

したがって，平均化によりマークが互いに相殺し合うようなマークの組にする，あるいは，平均の結果がそれぞれのマーク検出に対して十分小さいものであれば，各フレームのマークを一律に破壊することは困難である．また，ランダム系列が不明な抽出側で，同一のマークの埋め込まれているフレームを選んで平均をとることは試行の組合せ数が非常に大きいので，したがって，マークのランダム選択の導入により，マークの不正除去は困難となる．

3.3 フレームのランダム分割

マークがいくつかの基本要素（マーク要素）の組み合わせで構成されているとき，画像をその要素サイズに分割して部分的にマーク要素を測定すると，単一の領域では前節の方法により，どのマーク要素が適用されているか判断することは困難だが，二つの領域の間には統計的に相関が現れる．マーク要素の 種類をnとすると，ある２箇所にはn^2のうちm通り以下の組合せしか現れないからである．したがって，２箇所の相関をフレーム全体でとって，その組合せを調べると，前節で利用したm種類のマークが判明する．m種類のマークが判明すれば，それらをひとつずつ各フレームから差し引いてみることにより，マークの反応のなくなったものが，そのフレームに埋め込まれていたマークであることがわかる．

この問題を解消するためには，画像を基本要素の単位でランダムに二つの集合に分けて，それぞれにマークを埋め込む方法をとれば良い．その結果，ある２箇所にはn^2のうちm^2ほどの組合せが現れることになるので，nとmとが同程度の大きさであれば，その２箇所に明らかな相関が現れることがないからである．

なお，二つの集合の分け方が不明な場合に，フレーム全体から正しくマークを抽出するためには，以下に示すように，一方のマーク検出オペレータが，他方の半分のマークに反応しないように直交性を持たせれば良い．

$$\begin{aligned} O_{M_i}(R_h(M_j)) &> T/2 \quad (i=j) \\ &< T/2 \quad (i \neq j) \end{aligned}$$

ここで，$R_h(M)$はマーク要素を単位にMの半分をランダムに選択する関数であるとする．

参考文献

[1] Jian Zhao, et al.: “Embedding robust labels into images for copyright protection”, In Proc. of the Int. Congress on Intellectural Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, August 1995

[2] 沼尾他: “データハイディングによるデジタル署名技術”, In Proc. of IPSJ 53th annual conference, 1996

[3] 小林他: “データハイディングにおける圧縮耐性の基礎理論”, In Proc. of IPSJ 55th annual conference, 1997