結託耐性符号の実用化に向けた符号長の短縮

Collusion-Secure Fingerprinting Codes for Fair Content Distribution

磯谷　泰知　　村谷　博文
■ ISOGAI Taichi　■ MURATANI Hirofumi

デジタルコンテンツの不正な流通を防ぐ技術の一つに電子指紋方式（Digital Fingerprinting）がある。これは，個々のコンテンツにユーザーID(Identification）を埋め込んでおき，不正に流通したコンテンツのIDから不正者を特定する技術である。複数の不正なユーザーがコンテンツを比較し埋め込まれているIDを書き換える結託攻撃に備えるため，この方式では，通常のIDの代わりに“結託耐性符号”を用いる。しかし，従来の結託耐性符号では，結託攻撃による不正者の見逃しやえん罪を防ぐために，符号長を極めて長くする必要があった。

東芝は，不正者追跡アルゴリズムの見直しや最適化などにより，結託耐性符号の符号長をこれまでの1/15 ～ 1/20へと削減し，実用化にめどをつけた。

Digital fingerprinting is one of the techniques employed to prevent illegal distribution of digital contents. In the case of illegal distribution, pirate users can be traced and identified from each user's ID embedded in the digital contents. In a digital fingerprinting system, collusion-secure codes are often used instead of common IDs to control infections by pirate users rewriting their IDs. However, conventional collusion-secure codes require very long code lengths in order to prevent failure to trace pirate users as well as the possibility of false charges.

Toshiba has developed a technique that can reduce the length of collusion-secure fingerprinting codes to about 1/15 to 1/20 compared with the conventional code length by improvement of the tracing algorithm and other optimizations, and is promoting the practical application of a digital fingerprinting system incorporating this technique.

1　まえがき

近年，映像や音楽コンテンツのデジタル化が進み，非常に低コストでコピーが行えるようになってきている。デジタル化が進むことで，デジタルコンテンツのコピーを不正に配布することによる著作権侵害が深刻化しており，対策が急務となっている。

このようなデジタルコンテンツの不正な配布を防ぐ著作権保護技術として，電子透かし技術（Digital Watermarking）がある。電子透かしは，デジタルコンテンツに対して，人に知覚できないレベルの微小な変更を加えることで，コンテンツと不可分な形で付加情報を埋め込む技術である。そのため，電子署名や暗号化と異なり，アナログ化しても付加情報が残ることが特徴である。

電子透かし技術を用いた著作権保護方式は，大きく二つの手法に分けられる。一つはコピー制御（Copy Control）と呼ばれるもので，コンテンツをDVDなどに記録する際に“複製可能（Copy Free）”や“複製不可（Copy Never）”などの情報を埋め込んでおき，再生機器側でコピー制御情報を読み出してコンテンツの流通を制御する方式である。もう一つは電子指紋方式（Digital Fingerprinting）と呼ばれ，コンテンツに配布先ユーザーのID情報を埋め込むものである。

ここでは，これらのうち電子指紋方式を取り上げ，埋め込み情報から不正にコンテンツを流通させた犯人を追跡する手法と，そこで利用される符号の実用化に向けて東芝が改良した結果について述べる。

2　電子指紋方式の概要

電子指紋方式は，ネットワークを介してユーザー個々にコンテンツを配布する，VOD（ビデオ オン デマンド）のようなサービス向けの著作権保護方式である（**図1**）。具体的には，配布するコンテンツの一つひとつに電子透かし技術を用いてユーザー個別のIDを埋め込む。これにより，コンテンツが不正に流通した際に，コンテンツに埋め込まれたユーザーIDを基に不正者を特定できるようになる。

しかし，電子指紋方式では，複数のユーザーが異なるIDを埋め込まれたコンテンツを持ち寄り，それらの差異を書き換える結託攻撃への対策が必要となる。結託攻撃が行われると，もともと埋め込まれていたIDが書き換えられてしまうため，不正者を特定できないだけでなく，正当なユーザーが告発されるおそれもある。

結託攻撃に備えるため，電子指紋方式では通常のIDを用いるのではなく，はるかに多くの冗長性を持つ符号（mビット

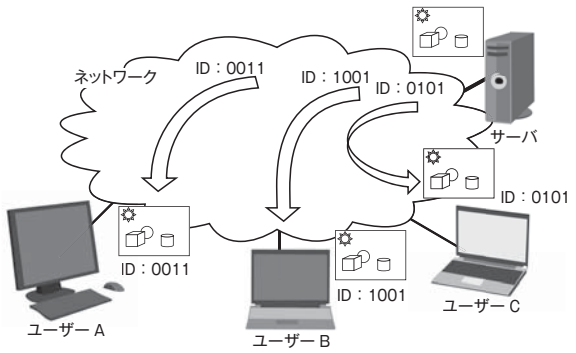

図1. 電子指紋方式のVODへの適用 — 各ユーザーにコンテンツを配信する際にID情報が埋め込まれる。

Fingerprinting method for video on demand

の1，0系列）がIDとして用いられる。

3　結託攻撃のモデル

結託攻撃とは，不正な複数のユーザーが固有の符号が埋め込まれたコンテンツを持ち寄り，それぞれの相違点を書き換えることによって，埋め込まれたIDを無効化しようとする攻撃である（**図2**）。

すべての結託者間で符号の値が一致している箇所は，コンテンツ上の電子透かしも一致しているため，コンテンツをどのように変更すれば符号のシンボルを変えられるのか攻撃者にはわからない。このことから結託攻撃には，結託した攻撃者の符号の中で，同じ位置にあってシンボルが異なる場合にしか，その符号のシンボルを書き換えられないという制約が生じる。

この制約を，符号の観点から**図3**に例示する。ユーザーAは符号“0000 0000”を，ユーザーBは符号“0000 0011”を，

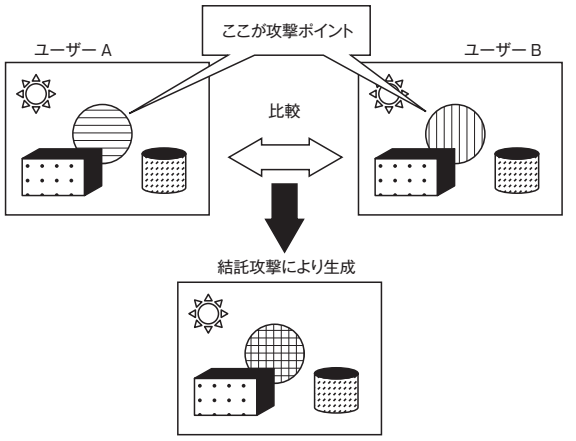

図2. 結託攻撃の対象 — コンテンツの相違点にID情報が埋め込まれていることが推測でき，相違点を書き換えることで，ID情報が無効化される。

Collusion attack

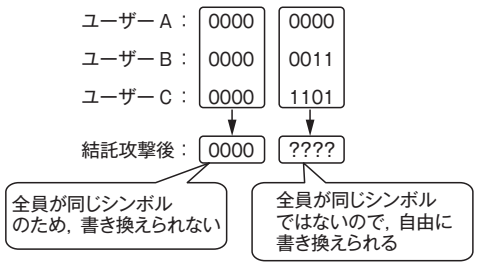

図3. 結託攻撃の制約 — 全員が同じシンボルの場合は書き換えられないが，ひとりでも違うシンボルの場合は書き換えられる。

Restriction of codes in collusion attack

及びユーザーCは符号“0000 1101”を持つものとする。3人の符号の前半4ビットは全員が“0000”であるため，結託攻撃の制約によってこの部分は書き換えられず，結託攻撃後の符号も必ず“0000”となる。一方，後半の4ビットについては全員のビットが一致していないので，結託者の好きなようにシンボルを変更できる。

4　結託耐性符号による不正者の特定

3章で述べたように，電子指紋に対する結託攻撃では，攻撃者にいくつかの制約があり，埋め込まれた任意のシンボルを任意の値に書き換えることは容易ではない。

結果として，結託攻撃によって書き換えられた後の符号は，結託に荷担したユーザーのうち，少なくともひとりの符号と強い相関（関連性）を持つことになる。結託耐性符号は，このことを積極的に利用して不正者を特定するものである。

結託耐性符号を用いて，不正に流通しているコンテンツから結託者を特定する手順を**図4**に示す。管理者は，まず不正に

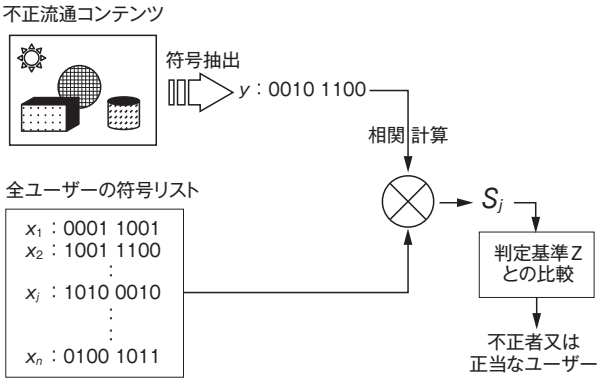

図4. 不正者を特定する手順 — 不正に流出したコンテンツから抽出した符号と各ユーザーの符号の相関を計算し，しきい値Zとの大小判定により不正者を特定する。

Process of identification of pirate users

流通したコンテンツから，埋め込まれている符号yを抽出する。yはm次元のベクトルで，その要素は0又は1のシンボルである。一方で管理者は，当該コンテンツを配布した際に埋め込んだ符号のリストからユーザーjの符号x_jを得て，(1)式によりyとの相関を計算し，これをユーザーjの点数S_jとする。

$$S_j = \sum_{i=1}^{m} y_i \left(x_{ji} - \overline{x_i}\right) / \sigma_{x_i} \qquad (1)$$

ここで，y_iは結託攻撃後の符号のiビット目のシンボル，x_{ji}はユーザーjのiビット目のシンボル，$\overline{x_i}$及びσx_iはiビット目のシンボルにおける“1”の期待値と標準偏差である。

このように計算されたS_jの頻度分布を模式的に示したのが**図5**である。S_jが大きい値を持つユーザーほど，犯人である可能性が高く，適当な判定基準Zを設けてS_j>Zとなるユーザーjを結託への荷担者と判断する。

図5において，ε_1はすべての不正者を正当なユーザーと誤る確率であり，ε_2は正当なユーザーを不正者と誤る確率である。結託ユーザーの人数がc人以下であれば，これら2種類の誤りの一方でも起こる確率がε以下になるような結託耐性符号を特にc-secure符号と呼ぶ。

G. Tardosは，c-secure符号の性質を持つTardos符号を開発したが[1]，その符号長は極めて長く実用的ではないという問題があった。

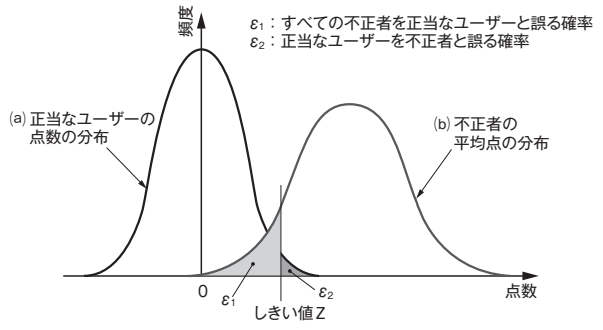

図5．不正者の平均点と正当なユーザーの点数の分布 — 両者の分布の違いによって不正者を特定する。
Distributions of scores

5　Tardos符号長の短縮による効果

当社は，後述する改良によって，Tardos符号の符号長を，1/15～1/20程度に短縮した。具体的な符号長を**表1**に記す。

改良した符号長を基に応用例を考えてみる。多くの映像コンテンツは30フレーム/sであるので，2時間の映像コンテンツに対して，映像用電子透かし技術を用いて結託耐性符号を埋め込むことを想定すると，総フレーム数は2.16×10^5フレームである。結託者数を32人とした場合，1ビット/フレームを切る符号の埋込み量となる。また，結託者を4人とすれば，3,400ビット程度で符号が構成できるので，20 minの映像コンテンツ(36,000フレーム)では，0.1ビット/フレームを切る(**表2**)。

通常，電子透かし技術においては，再圧縮やフレーム除去，切出しなどが行われても透かし情報を正しく抽出できる方式とするため，透かし情報を冗長に埋め込んでおく必要がある。このため，1ビット/フレームは必ずしも容易な埋込み量ではない。しかし，符号の埋込みに適した電子透かしアルゴリズムと組み合わせれば実現できるレベルに達しており，当社が行った改良によって十分実用的な符号長が達成されたと言える。

表1．改良方式の符号長とTardos符号長の比較
Comparison of code lengths of newly developed method and Tardos's method

項　目	結託者数（人）				
	4	8	16	32	64
① 改良方式の符号長（ビット）	3.36×10^3	1.36×10^4	5.29×10^4	2.04×10^5	7.85×10^5
② Tardos符号長（ビット）	5.60×10^4	2.24×10^5	8.96×10^5	3.58×10^6	1.43×10^7
①/②　（%）	6.00	6.06	5.91	5.69	5.48

表2．映像コンテンツへの符号の埋込み例
Example of embedding of codes into video contents

映像時間（min）	結託者数（人）	埋込み量（ビット/フレーム）
120	32	1
20	4	0.1

6　Tardos符号の改良法

ここでは，符号長を短縮するために行った改良[2]について述べる。

符号長の短縮には，五つのポイントがある。

(1)　追跡アルゴリズムの改良
(2)　不正者をひとりも追跡できない確率ε_1の厳密評価
(3)　えん罪発生確率ε_2の厳密評価
(4)　誤り確率の割合の最適化
(5)　符号の生成確率の最適化

ここで述べる手法を採用することで，**図6**や**図7**のように，正当なユーザーと不正者の二つの分布を識別しやすくするとともに，符号長をもっとも短くできるしきい値Zを定めた。以下に，それぞれの改良内容について述べる。

(1)　追跡アルゴリズムの改良　　図6のように，不正者の平均点の分布をより右側にずらすことで，二つの分布を識別しやすくするものである。具体的には，不正者を判定す

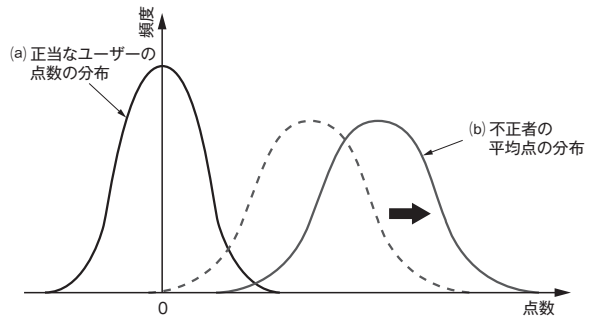

図6. 改良による分布の変化1 — 追跡アルゴリズムの改良及び符号の生成確率の最適化を行った場合，不正者の平均点の分布が右側に移動する。これを不正者の識別に用いる。

Transformation of distribution by improvement 1

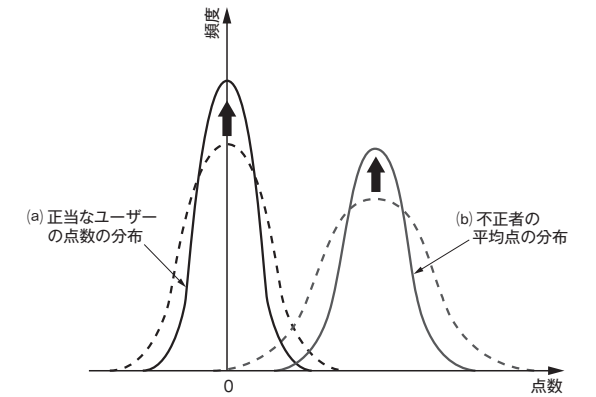

図7. 改良による分布の変化2 — 不正者をひとりも追跡できない確率及びえん罪発生確率の厳密評価を行うと，分布の広がりを小さくできる。これにより，不正者の識別を容易にする。

Transformation of distribution by improvement 2

る点数の計算方法を(2)式に置き換える。

$$S'_j = \sum_{i=1}^{m} (2y_i - 1)(x_{ji} - \bar{x_i}) / \sigma_{x_i} \qquad (2)$$

このようにすることで，図6(b)のように，不正者の平均点の分布を右側にずらすことができるようになり，二つの分布をより識別しやすくなる。(1)式による評価では，y_i=1の場合しか評価されていないのに対して，(2)式ではy_i=0とy_i=1の両方が評価されている。

(2) 不正者をひとりも追跡できない確率ε_1の厳密評価
Tardosの符号構成法における確率の評価を更に厳密に行うことで，図7(b)のように不正者の分布の広がり（分散）を小さくし，二つの分布の識別を容易にする。その結果，同じ誤り確率をより短い符号長で達成することができる。

(3) えん罪発生確率ε_2の厳密評価　(2)と同様に，Tardosの評価を更に厳密に行うことで，図7(a)のように正当なユーザーの点数の分散を小さくする。これにより，同じえん罪発生確率を設定した場合，Tardos符号より短い符号長で達成できる。

(4) 誤り確率の割合の最適化　ε_1とε_2の値においてもっとも符号長が短くなるように，しきい値Zの値を決める。条件としては，$\varepsilon \geqq \varepsilon_1 + (n - c)\varepsilon_2$を満たせばよいが，Tardosの符号構成法では$\varepsilon_1 = \varepsilon_2 = \varepsilon / n$と定めていた。このように定めたのは証明のしやすさのためであり，実際には符号長を最小にする値を論理的に求めることができる。

(5) 符号の生成確率の最適化　符号の生成確率を変化させると，iビット目における不正者の平均点の期待値が変化するので，不正者の平均点の分布の山が左右にずれる。符号長を短くするためには図6(b)のように，この分布の山をできるだけ右側に移動させられるよう符号の生成確率を定めればよい。現時点では，結託者が多い場合の最適な符号の生成確率は理論的に求められていないので，数値解析により，もっとも符号長を短くできる符号の生成確率を導出する。

7　あとがき

当社は，Tardosの符号構成法を基に符号長を短縮し，従来の符号長に比べ，1/15～1/20とすることができるようになった。今回の符号長の短縮によって，電子透かし技術と結託耐性符号を融合させた，電子指紋方式の実用化に大きく近づくことができた。

今後は，電子指紋方式に適した電子透かし技術の開発を進めていく。

文　献

(1) Tardos, G. "Optimal Probabilistic Fingerprinting Codes". J. ACM. **55**, 2, 2008, p.1－24.
(2) 磯谷泰知，ほか．符号生成確率分布および追跡アルゴリズムの改良によるTardos符号の短縮．信学技報．ISEC2007-85，**107**，209，2007，p.85－90.

磯谷　泰知　ISOGAI Taichi
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。情報セキュリティ分野の研究・開発に従事。情報理論とその応用学会会員。
Computer & Network Systems Lab.

村谷　博文　MURATANI Hirofumi, D.Sc.
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主任研究員，理博。暗号技術及び暗号応用システムの研究・開発に従事。電子情報通信学会，情報処理学会，IEEE会員。
Computer & Network Systems Lab.