電子化知的財産・社会基盤 15－8
（２００２．２．１６）

切り取り耐性を強化したLCSD個体化方式

高橋 由泰　青木 輝勝　安田 浩

東京大学 先端科学技術研究センター

{takahasi, aoki, yasuda}@mpeg.rcast.u-tokyo.ac.jp

ディジタルコンテンツの不正流通を防止するための方策として電子透かしを用いる方法がよく使われているが，電子透かしはマルチキャストネットワークでは使用しにくいという大きな問題がある．それはマルチキャストネットワークでは同一の透かしが入ったコンテンツが全ユーザに配信されるため，購入者の特定ができないからである．
このような問題を解決する新しいメタデータ記録方式として我々は既に「LCSD: 階層化コンテンツ超流通システム」を提案している．この方式はマルチキャストネットワークにおいて安全にメタデータをコンテンツに記録できるという利点を持つが，従来画像の一部切り取りに対する耐性の弱さがあった．
我々はこの耐性を改善したLCSDのための新しい個体化方式を考案したので報告する．

キーワード: LCSD　個体化　電子透かし

LCSD Individuating Method Robust against Cropping

Yoshiyasu Takahashi　Terumasa Aoki　Hiroshi Yasuda

Research Center for Advanced Science and Technology, the University of Tokyo

In recent years, an illegal distribution of digital contents is becoming a serious problem. In order to prevent such illegal distribution, digital watermark is often used. However, it cannot be used in multicast networks, because the same contents is delivered to many users. Many users watching the same contents, it is impossible to discover to whom the content has delivered by the embedded watermark.
To solve this problem, we have already proposed the LCSD individuating method. It is, like digital watermark, the method to incorporate the meta-data to the contents, but it is suited to the multicast networks.
However the existing LCSD individuating method is not robust against the cropping of the contents. In this paper, we propose another individuating method for LCSD robust against the cropping of the image.

Keywords: LCSD　individuating　digital watermark

1 はじめに

近年コンテンツ産業の市場規模が大きく伸びている．日本マルチメディアフォーラムの報告 [4] によれば，日本のコンテンツ産業の市場は 1995 年で 158 億円であり，2005 年には 234 億円に達すると予測されている．

このように市場が成長する一方で，不正流通の問題が大きな問題となりつつある．特に近年は以下のようなユーザが不正流通をやりやすいような環境が整えられてきており，不正流通の防止技術の要求はますます高まっている．

- 高速なネットワーク

  インターネットへのアクセス速度は家庭においても低廉化と高速化が急速に進んでいる．これはインターネット接続業者間の競争が激しくなったことが大きな要因となっている．

  特にここ一年の大きな動きとしては、家庭用の 1Mbps から 4Mbps 程度の実効速度のアクセス網が急速に普及したことが挙げられる．総務省発表の資料 [5] によれば，家庭用高速回線である CATV 加入者数と DSL 加入者数の推移は図 1 に示すとおりであり，特に DSL 加入者数は 2000 年 12 月末から 2001 年 12 月末までの 1 年間で約 157 倍の 152 万加入に到達した．

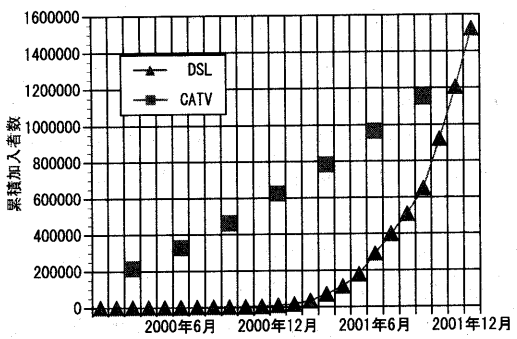

図 1: CATV, DSL 加入者数の推移

また，総務省発表の資料 [6] では，今後の高速・超高速インターネットの普及予測（実加入世帯ベース）は表 1 に示すとおりであり，当面は DSL が高速・超高速インターネットアクセスの主流を占めるが，光ファイバ網を活用した超高速インターネットが 2003 年度から急速に普及し，2005 年度には DSL を逆転するものと予測されている．

- コンテンツ圧縮技術の進歩

  ディジタルコンテンツの圧縮技術の進歩も，不正流通への懸念を増大させている．オーディオコンテンツの圧縮フォーマットとして MP3 が広く使われているが，この形式では一般に 1.4Mbps の CD 品質音声データを，その品質をほとんど損なうことなく 128kbps への圧縮が可能である．圧縮率は 1/10 に達する．また，最近の圧縮技術では同程度の品質を 80kbps で達成できる．動画像では MPEG-2 や MPEG-4 があり，MPEG-4 では NTSC をやや下回る程度の品質の動画像を 1 ないし 2Mbps 程度のビットレートで記録することができる．

- P2P の普及

  P2P (Peer to Peer) は WWW 同様，不特定多数間でのファイルの流通を可能とする技術であるが，P2P と WWW とでは，WWW がクライアント–サーバモデルに基づいてサーバを必要としているのに対し，P2P は本質的にはサーバを必要としないという違いがある．これは P2P では各ユーザの計算機がそれぞれクライアントとサーバの両方の役割を担えるよう設計されているためである．P2P ではサーバを必要としないため匿名性が高く，ファイルの不正流通の温床になっているとの批判がある．

これらの技術を使用すれば，ディジタルコンテンツの不正流通は非常に簡単に行うことができる．現在，4 分程度の音楽であれば，送受信には 15 秒程度で行うことができ，2 時間の映画でも，1 時間程度で送受信できる．また，100Mbps 程度のネットワークが普及すると予測されている 2005 年度には，2 時間の映画の送受信には 2 分以内に終わると予測される．

		2001年度	2002年度	2003年度	2004年度	2005年度
高速	DSL	164	481	749	722	695
	CATV	205	323	383	417	429
	無線	2	16	41	65	80
超高速	光ファイバ	7	97	335	593	773
総計		378	917	1,513	1,797	1,977

表 1: 高速・超高速インターネットの普及予測（単位:万世帯）（総務省 [6]）

このように，不正流通が極めて手軽にできるようになった結果，音楽では Napster 等で既に不正流通が非常に大きな問題となった．また映画においても，同様に不正流通が問題となる危険性が指摘されている．

2 ディジタルコンテンツの著作権管理手法

ディジタルコンテンツの著作権を管理・保護するために，コンテンツの暗号化やコンテンツへの電子透かしの埋め込みといった手法が一般に用いられる．

2.1 暗号化

ディジタルコンテンツは暗号化されて配布されることが多い．暗号化によって，配布途中で盗聴その他の手段によって配布データが販売者・購買者以外の第三者に渡ったとしても，ディジタルコンテンツそのものが第三者に渡ることを阻止することができる．このように暗号化によってコンテンツの安全な一時配布が可能となる．

一方で暗号化ではディジタルコンテンツの二次不正流通を防止することはできない．これは暗号が一旦解除されれば，もはやディジタルコンテンツを守るものがなくなるため，正規購買者がディジタルコンテンツの二次不正流通を行うことを防ぐことができないからである．

2.2 電子透かし

ディジタルコンテンツの二次不正流通を防止するために現在広く行われている方法が電子透かしの埋め込みである．

電子透かしとは，情報を人間には知覚できないような形でコンテンツそのものに埋め込む手法である．電子透かしは人間に知覚されないよう，多くの場合ノイズのような形で埋め込まれる．

電子透かしを著作権保護に利用する場合，コンテンツのメタデータをコンテンツ自身に埋め込む．埋め込むメタデータとしては，著作者情報なども考えられるが，本稿が対象とする二次不正流通防止の目的では，一般に購入者情報を埋め込む．

電子透かしは，サーバ側埋め込みとユーザ側埋め込みの二つの方式に分類することができる．

- サーバ側埋め込み

  電子透かしをコンテンツの配信サーバで埋め込む方法．ユーザには既に電子透かしを埋め込んだファイルが配布される．

- ユーザ側埋め込み

  電子透かしをコンテンツの購入者の計算機で埋め込む方法．ユーザには電子透かしを埋め込んでいないファイルが配布され，インストールプログラム等によって，コンテンツに電子透かしが埋め込まれる．

2.3 電子透かしの問題点

電子透かしには，マルチキャストネットワークに適用しにくいという問題点が存在する．

マルチキャストネットワークでコンテンツを配信する場合，電子透かしのサーバ側埋め込みは不可能である．これはサーバ側で透かしを埋め込んだ場合，各ユーザに同一のファイルがマルチキャストで配信されるため，各ユーザが同一のコンテンツを視聴することになってしまう．このため，各ユーザが同一の電子透かしを割り当てられてしまうため，ユーザの特定ができないことによる．

一方で，電子透かしのユーザ側埋め込みはマルチキャストネットワークでコンテンツを配信する場合にも用いることができる．それはユーザ側で電子透かしを埋め込むので，同じファイルをマルチキャストで配信しても，各ユーザに別の電子透かしを割り当て，各ユーザが別のコンテンツを視聴するように操作することが可能だからである．

しかしながらこの方法にもソフトウェアの安全性に関する問題がある．電子透かしを埋め込むソフトウェアをユーザの計算機で実行させるため，そのソフトウェアがユーザに解析されてしまう危険性がある．この時問題となるのは，この方法では電子透かしが入っていないコンテンツにユーザ側で電子透かしを埋め込むため，ソフトウェアを解析され，電子透かしが入っていないコンテンツを取り出し，電子透かしは挿入しないように解像されてしまう危険があることである．

3 LCSD個体化方式

我々は，前節で述べたマルチキャストでは電子透かしが使いにくいという問題を解決する新しいメタデータ挿入法であるLCSD個体化方式を既に提案している [1] [2] [3] .

3.1 LCSD個体化方式の概要

LCSD個体化方式は，静止画像に対し電子透かし同様メタデータを埋め込む方式である．その特長としてマルチキャストネットワーク環境において，プログラムが解析されてもメタデータが入っていないコンテンツが流出しないという点が挙げられる．

LCSD個体化方式では実際にメタデータそのものをコンテンツに埋め込むのではなく，コンテンツの各視聴者毎にコンテンツを変形させるということにより情報を埋め込む．各視聴者毎にコンテンツを僅かに変形させ，各視聴者の視聴するコンテンツが個体として他と区別できるようにしてあるので，コンテンツと視聴者の1:1対応の関係から，メタデータを埋め込むのと同じ効果が得られる．

LCSD個体化方式の基本処理を，図2に示す．まず静止画像をまずオブジェクト毎に分割する．その後同じオブジェクトのコピーを複数用意し，それぞれのコピーがお互いに異なるようにオブジェクトの個体化を行う．それらを再構成することにより，視聴者用のコンテンツを得ることができる．

この方法では，視聴者毎のコンテンツの違いは，各オブジェクトの違いの組み合わせによって得られる．例えば図2では，5個のネクタイと5個のビールを用意した．人物は複数個用意することはしなかった．この結果再構成後のコンテンツとしては，$5 \times 5 = 25$ 通りの組み合わせが存在することになり，これが視聴者毎のコンテンツの違いとなる．すなわち，この場合の最大視聴者数は25人ということになる．

3.2 LCSD個体化方式の利点

LCSD個体化方式は，マルチキャストネットワークに用いることができるという大きな利点を持っている．

LCSD個体化方式では，それぞれオブジェクト個体化が済んだ全てのコピーをマルチキャストでコンテンツ視聴者に送付する．このとき全てのコピーをそれぞれ別の鍵で暗号化しておく．すなわち一つのコンテンツに対して，全オブジェクトの全コピーの数の鍵を用いることになる．

コンテンツの購入を希望するユーザには，各オブジェクト毎に一つ鍵を選び，オブジェクト数と同数の鍵をユニキャストにて送付する．よってユーザは，それぞれのオブジェクトについてただ一つのコピーのみを復号化できる．他のコピーは異なる暗号で暗

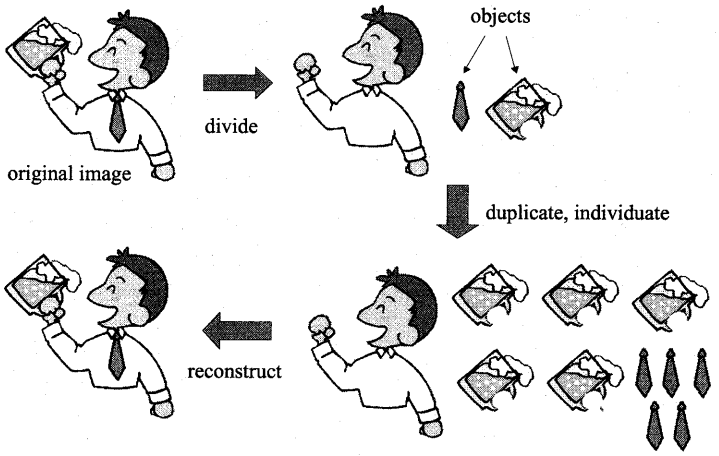

図 2: LCSD 個体化方式の概要

号化されているため復号化できない．その結果ユーザはマルチキャストで受信した全てのデータを復号化することはできず，ある特定の個性を持ったオブジェクトだけを復号化することができる．

ここでの利点は，コンテンツの復号化と同時にコンテンツの個体化が完了するため，電子透かしのユーザ側挿入とは異なり，処理を切り離される心配がないことである．

また，電子透かしのサーバ側挿入とは異なり，マルチキャスト通信に適用可能である．画像をオブジェクトに分割したことで，購入者数はオブジェクト毎の個性の組み合わせで決まるため，オブジェクト数を 10，それぞれのオブジェクトのコピー数を 10 とすれば $10^{10} = 100$ 億 という膨大な個体を作ることができる．それでいて，実際の通信での通信量は，各オブジェクトの総和を全体の 10% とし，それぞれのオブジェクトのコピー数を 10 と仮定すれば，約 2 倍の通信量で済む．

各オブジェクト毎に復号化されるコピーは一つだけであり，残りは全て復号されず不要なデータであるから，各ユーザで受信するファイル容量はオリジナルコンテンツよりも多いのは確かであるが，約 2 倍で済んでいる．マルチキャストを使えるためにサーバ側の計算機資源やネットワーク資源に負担を与えず，将来の動画像配信への応用が有望である．

3.3 LCSD オブジェクト個体化

LCSD 個体化方式では，各オブジェクトのコピーの個性化はいろいろな方法が考えられる．我々は今までに 2 つの方式を提案した．

- 位置ずらし法

  位置ずらし法は画像をオブジェクトに分割し，それぞれのオブジェクトの位置を 1 画素など微少量ずらす方法である．画像の個性は，個々のオブジェクトの位置を検査することによって判断する．例を図 3 に示す．この図では時計や汗の位置をずらしている．説明のため一目で分かるくらい大きくずらしているが，実際にはこの図ほど大きくずらすことはしない．

  この方法は，利用するオブジェクトが位置をずらしても不自然さを感じないようなものに限られることから，自然画像を自動的に処理するという場合には適用が難しい．

- 複数透かし法

  複数透かし法は，図 4 に示すように，画像をいくつかのオブジェクトに分割した後，それぞれのオブジェクトに別の電子透かしを挿入

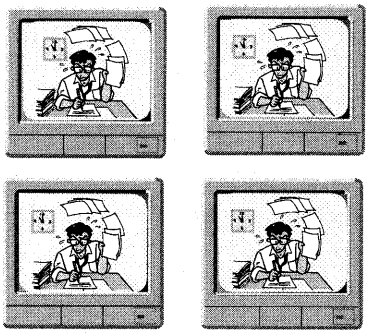

図 3: 位置ずらし法

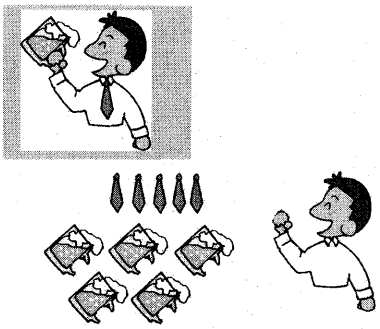

図 4: 位置ずらし法

する方法である．個々のオブジェクトは埋め込まれた電子透かしによって区別する．

埋め込む電子透かしそのものは，オブジェクトの区別がつけられることのみが要求条件であり，特に種類を選ばない．よって画素置換型，周波数領域型の両方が使え，また将来より良い電子透かし法が開発されれば，それを使うこともできる．

また，複数透かし法の場合，オブジェクトの分割方法の制限も緩やかである．位置ずらし法の場合では，例え微少変位とはいえ，画像内の例えば椅子などのオブジェクトを二つに分割して変位させると画像が変化していることを知覚できてしまうが，複数透かし法の場合は，埋め込む電子透かしの性質によっては例え椅子などのオブジェクトを二つに分割しても知覚できるほどの違いを生じさせないことが可能である．

以上，画像をオブジェクトに綺麗に分割できなくても使用可能であることから，複数透かし法は位置ずらし法ではできなかった自然画像へ適用することができる．また，イラストにおいても，既にビットマップ形式になってしまったものなど綺麗なオブジェクトへの分割が難しい画像に対しての応用も有望である．

3.4 切り取り耐性を強化した LCSD オブジェクト個体化方式の提案

図 2 のようなオブジェクト分割では，画像の一部切り取り処理に対する脆弱性が存在する．例えば図 2 においてビールを切り取られ，人間だけのコンテンツを作られたとき，その人間のコンテンツだけでは購入者の特定までは至らない．これは，画像の個性は各オブジェクトの組み合わせによっているため，ビールの個性が分からない時点で購入者が特定できなくなってしまうことによる．

我々はこの問題を解決する新たな LCSD におけるオブジェクト個体化方式として，ビットプレーン法を考案した．

この方式は画像をビットプレーンに分割し，各ビットプレーンをオブジェクトと捉えそれぞれのビットプレーンを白黒画像用の電子透かしで個体化する方式である（図 5）．

例えば図 5 では，ある色深度 8bit の白黒画像のビットプレーンのうち第 2，第 4 プレーンを LCSD のオブジェクトとして用い，それぞれ 5 個の違う透かしが入ったプレーンを用意している．この結果，5×5 の 25 通りの違いを出せることになる．

ビットプレーンの違いを出すために実際に埋め込む電子透かしの方式としては，1 ビット白黒画像に埋め込める電子透かしであれば適用可能である．例えば図 6 に示すような画素置換型の電子透かし方式が考えられる．この透かし方式では，2×2 画素を 1 ブロックとし，そのブロック内に白と黒の画素が

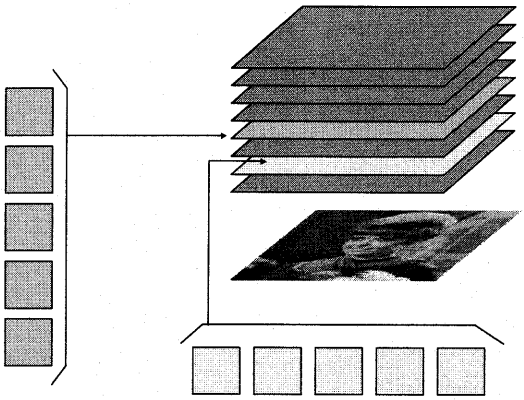

図 5: ビットプレーン法

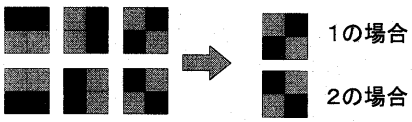

図 6: 1 ビット白黒画像への電子透かし

ちょうど 2 つずつ存在するようなブロックについて情報を埋め込んでいく．このとき埋め込み際し，埋め込む情報の 0/1 に合わせ，ブロックを図 6 に示すようなどちらかのパターンに変更する．

このような電子透かしを用いて，LCSD 個体化をした画像が図 7 である．ここでは，赤色の 8 枚のビットプレーンのうち，第 3 プレーンと第 5 プレーンを LCSD 個体化に使用するオブジェクトとした．それぞれ別の透かしを埋め込んだものを 2 つ用意し，それらを組み合わせた．この結果 4 枚のコンテンツが得られている．埋め込んでいる電子透かしがかなり基本的な電子透かし方式であるにも関わらず，得られるコンテンツの画像品質はかなり良好である．

カラー画像を用いる場合，ビットプレーンとして 24 枚ある．あまりにも低いビットプレーンに情報を埋め込むと，圧縮等によって情報が欠落する心配がある．一方であまりに高いビットプレーンに情報を埋め込むと，人間に近くされないように埋め込むことが難しくなる．よって中位のビットプレーンを，各色 2 枚程度使うのが現実的な解であると考えられる．

この場合，オブジェクトとしては 6 つある．購入者数を p 人と仮定すれば，必要な各オブジェクトのコピーの数 n は

$$n = \log_6 p$$

であり，100 万人に対しコピーは 8 枚，1000 万人に対しコピーは 9 枚必要になる．このときの各ユーザへマルチキャストにて送信されるデータ量は，100 万人時に原画像の 1.9 倍，1000 万人時には原画像の 2.1 倍で済み，実行可能と言える．

このビットプレーン法の他の個体化法に対する利点は，画像の切り取り処理に対する耐性があることである．切り取り処理は画素単位で行われる処理であるから，画素内のビットは必ず同じ処理を受ける．すなわち画素が切り取られる場合は画素内のビットは同時に切り取られ，画素が残る場合は画素内のビットも同時に残る．よって透かし情報が読みとれる程度の領域が残っていれば，電子透かしを読みとることができる．ここでいう透かし情報とは，同一オブジェクトの各コピーを区別することさえできればよいので，一般に 4 ビット程度であるから，試験実装で用いた透かし方式を用いた場合，32 画素程度の領域さえ残っていればコンテンツの個体を識別できることになる．

4 まとめ

本稿ではマルチキャスト通信に向いたメタデータ記録法である LCSD 個体化方式において，画像の一部切り取り処理にも耐性があるオブジェクト個体化方式であるビットプレーン法を提案した．

LCSD 個体化方式は将来の動画像配信で用いられることが有力視されているマルチキャストで使うことができるため有望な方式であるが，今までのオブジェクト個体化方式ではオブジェクトを切り取られると全体の情報が欠落してしまうため，オブジェクトが切り取られることがないようオブジェクトの配置を細かく調整する必要があった．

しかし本稿で提案したビットプレーン法を用いれば，画像の一部切り取り処理にも対応できるため，オブジェクトの配置を調整する必要はなくなり，手

図 7: ビットプレーン法による LCSD 個体化例

軽に LCSD 個体化方式を用いることができるようになった.

参考文献

[1] 高橋由泰, 青木輝勝, 安田浩, "階層化コンテンツ超流通システムにおける個性化方式, " 情報処理学会第 63 回全国大会 2X-03, 2001.

[2] 高橋由泰, 青木輝勝, 安田浩, "階層型コンテンツ超流通システム, " 情報処理学会電子化知的財産・社会基盤研究会研究報告 No.13 - 4, 2001.

[3] 高橋由泰, 青木輝勝, 安田浩, "階層化コンテンツ超流通システム LCSD における切り取り耐性を強化した個体化方式, " 情報処理学会第 64 回全国大会 5T-02, 2002.

[4] 日本マルチメディアフォーラム, "マルチメディアの現状と展望, " 1998.

[5] 総務省, "インターネット接続サービスの利用者数等の推移【平成 13 年 12 月】(速報), " 総務省報道発表資料, Jan. 2002.

[6] 総務省, "全国ブロードバンド構想～「世界最先端の IT 国家」の実現に向けて～, " 総務省報道発表資料, Oct. 2001.

[7] 阿部剛仁, 藤井 寛, 串間和彦, 櫻井紀彦, "個別情報埋め込みにより管理機能を強化した画像流通方式," 信学論, Vol. J82-A, no.9, pp.1474–1482, Sep. 1999.

[8] 森 亮一, 河原正治, "歴史的必然としての超流通," 情報処理学会 超編集超流通超管理のアーキテクチャ シンポジウム論文集, vol. 94, no.1, pp.67–76, Feb. 1994.

[9] 森 亮一, "超流通の構造, 防御, 人々の利益—定義と基本式," 信学技報, ISEC94–13, Sep. 1994.

[10] 河原正治, "超流通における電子オブジェクト課金方式の検討," 信学技報, ISEC94–15, Sep. 1994.

[11] D.R.Stinson, 櫻井幸一監訳, "暗号理論の基礎," 共立出版, 1996.

[12] 松井甲子雄, "電子透かしの基礎, 森北出版, 1998.

[13] H. Berghel and L. O'Gorman, "Protecting Ownership Rights through Digital Watermarking," IEEE Computer , 29:7, pp. 101–103, 1996.