マルチメディア通信と分散処理　111－37
コンピュータセキュリティ　20－37
（２００３．２．２８）

著作権保護を考慮した画像コンテンツの配信システムに関する考察

蓮尾 知志*　　稲葉 宏幸*

概要　著作権保護対策を施したコンテンツ配信システムとして，暗号技術や電子透かし技術あるいはそれらを複合して用いたものなどが提案されている．従来のコンテンツ配信システムでは個人の不正コピーなどの不正行為に対してはよく検討されているが，複数ユーザの結託による不正行為についてはあまり検討されていない．そこで，複数のユーザが結託して構成された不正なコンテンツから，電子透かしとして埋め込まれたユーザID情報を利用して不正ユーザを割り出す一手法を提案する．また，このコンテンツ配信システムを用いることにより，ユーザ間のデータ譲渡を許しつつ著作権管理が可能な，データ分散共有型ファイル交換システムが構築可能となる．

Notes on Copyright Management for Digital Image Distribution System

Satoshi HASUO*　　Hiroyuki INABA*

abstract Many contents distribution systems with copyright management have been realized using by cryptography and/or fingerprint technology. However, few systems have examined a collusion problem. In this paper, first we propose a new algorithm which trace illegal users by using embedded user information from an illegal contents made by a collusion. Second, we show a new file exchange system with copyright management which permits data transfer between users.

1　はじめに

近年，FTTH網の充実などによる通信ネットワークの高速化や，情報記憶装置の大容量化などにより，それらを用いた音楽や動画などのコンテンツ配信が活発になってきている．それに伴い，不正コピーを抑止する等の著作権保護対策が重要な課題である．

従来のコンテンツ配信システムでは個人の不正コピーなどの不正行為に対してはよく検討されているが，複数ユーザの結託による不正行為についてはあまり検討されていない．そこで，複数のユーザが結託した場合でも不正ユーザを割り出す一手法を提案する．また，このコンテンツ配信システムを用いることにより，ユーザ間のデータ譲渡を許しつつ著作権管理が可能な，データ分散共有型ファイル交換システムが構築可能となることを示す．

*京都工芸繊維大学 工芸学部 電子情報工学科
*Department of Electronics and Information Science, Kyoto Institute of Technology

2　コンテンツ配信システム

以下にこれまでに提案されているいくつかの配信システムと，その問題点について述べる．

2.1　コンテンツ配信システム

A. [暗号技術による配信システム]
本システムでは，コンテンツ提供者であるプロバイダとユーザの間では，以下のようなやり取りが行われる．

(A-i) プロバイダは暗号化されたコンテンツをユーザに配布する．

(A-ii) ユーザはそのコンテンツに関してプロバイダと購入契約をかわす．

(A-iii) プロバイダは手順 (A-i) で暗号化されたコンテンツの復号鍵を，安全に伝送できる回線によりユーザに配信し，その復号鍵により暗号化コンテンツを復号することで，ユーザは完全なコンテンツを得る．

B. [電子透かしによる配信システム]
本システムではコンテンツ提供者であるプロバ

イダとユーザの間で，以下のようなやり取りが行われる．

(B-i) プロバイダは評価用のコンテンツをユーザに配布する．

(B-ii) ユーザがそのコンテンツに関してプロバイダと購入契約を交わす際に，ユーザはディジタル署名付の ID 情報等をプロバイダに送付する．

(B-iii) プロバイダは ID 情報等の透かし情報が埋め込まれたコンテンツを，安全に伝送できる回線によりユーザに配信する．

C. [阿部らによる配信システム [1]]
阿部らによって，暗号技術および電子透かしによる配信システムの長所のみを組み合わせたコンテンツ配信システムが提案されている．本システムではコンテンツ提供者であるプロバイダとユーザの間で，以下のようなやり取りが行われる．

(C-i) プロバイダは，暗号化されたコンテンツをユーザに配布する．

(C-ii) ユーザがそのコンテンツに関してプロバイダと購入契約を交わす際に，ユーザはディジタル署名付の ID 情報をプロバイダに送付する．

(C-iii) プロバイダは手順 (C-i) において生成された暗号化コンテンツに対して，オリジナルコンテンツに復号するための復号鍵とユーザの ID 情報を結合した ID 鍵を作成し，安全に伝送できる回線により ID 送付鍵を配信する．

(C-iv) ユーザがその ID 送付鍵を用いて，暗号化コンテンツを復号することにより，ID 情報などの透かし情報が埋め込まれたコンテンツが生成される．

D. [角野らによる配信システム [2]]
角野らによって，デコーダの耐タンパ性を必要としないコンテンツ配信システムが提案されている．以下ではこの配信システムを KIK-CDS と呼ぶ．本システムではコンテンツ提供者であるプロバイダとユーザの間で，以下のようなやり取りが行われる．

(D-i) プロバイダは暗号化されたコンテンツをユーザに配布する．

(D-ii) ユーザがそのコンテンツに関してプロバイダと購入契約を交わす際に，ユーザはディジタル署名付の ID 情報をプロバイダに送付する．

(D-iii) プロバイダは手順 (D-i) において暗号化コンテンツに対する復号鍵に，ユーザの ID 情報を電子透かしとして埋め込みを行うことで ID 送付鍵を生成し，安全に伝送できる回線により ID 送付鍵を配信する．

(D-iv) ユーザがその ID 送付鍵を用いて，暗号化コンテンツを復号することにより，ID 情報等の透かし情報が埋め込まれたコンテンツが生成される．

2.2 コンテンツ配信システムの比較

暗号技術による配信システムでは，全てのユーザが同じコンテンツを得るので，ユーザによる不正コピー行為に対して無力である．一方，電子透かし技術による配信システムでは，ユーザによる不正コピー行為は抑止できるが，評価用コンテンツと透かし入りのコンテンツの双方を配信する必要があり，これらの配信情報量が暗号技術による配信システムの場合の 2 倍になってしまうという短所がある．

阿部らによる配信システムは暗号技術および，電子透かしによる配信システムの長所のみを組み合わせた配信システムであるため，配信情報量が少なく，ユーザの不正行為を抑止することが可能である．しかし，デコーダの耐タンパ性が破られると，ユーザによるオリジナルコンテンツの生成や埋め込まれるべきユーザ ID 情報の改ざん等の不正が行われてしまうという短所がある．

KIK-CDS ではコンテンツ復号鍵内にユーザ ID 情報を埋め込むため，情報量が少なくユーザの不正行為を抑止でき，耐タンパデコーダを必ずしも用いなくてもよい配信システムである．

3 複数ユーザの結託攻撃に耐性のあるコンテンツ配信システムの提案

2で述べたKIK-CDSでは，正当なユーザが得たコンテンツを複数個用いることで，コンテンツの追跡を不可能とするような不正行為である結託攻撃について検討されていなかった．そこでここではKIK-CDSを基本としたユーザの結託攻撃に耐性のあるコンテンツ配信システムの提案を行う．

3.1 提案するコンテンツ配信システムにおける透かし情報の埋め込みアルゴリズム

以下に提案するコンテンツ配信システムにおける透かし情報の埋め込みアルゴリズムを述べる．

(i) 原画像に対し周波数変換を行う．本考察では離散コサイン変換を用いた．

(ii) 周波数領域で高周波領域と低周波領域に分離する．

(iii) 高周波領域を暗号化する．本考察では高周波領域をいくつかのブロックに分割し，ブロック内のデータの値を互いに交換することにより実現した．

(iv) (iii)において暗号化した高周波領域に対し，透かし情報を埋め込む．本考察では(iii)において，ブロック化し，暗号化した高周波領域に対し，復号を行う場合を"1"，行わない場合を"0"として透かし情報とした．

(v) (iv)において透かし情報を埋め込んだ高周波領域と低周波領域を組み合わせる．

(vi) 周波数逆変換を行い，透かし入りの画像を得る．本考察では離散コサイン逆変換を用いた．

図1に提案方式のブロック図を示す．

図2に評価用コンテンツを，図3に上記のアルゴリズムに基づいて，透かし情報を埋め込んだ画像コンテンツを示す．評価用のコンテンツのSN比は32.1dB，透かし情報入りコンテンツのSN比は46.3dBとなっている．

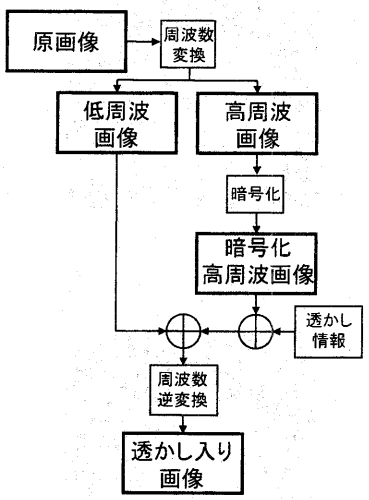

図1: 透かし情報の埋め込みアルゴリズム

3.2 ユーザの結託に対する透かし情報の耐性について

KIK-CDSや提案するコンテンツ配信システムにおいて配信されるコンテンツは，画像を周波数変換し，ブロック化した後，暗号化している．プロバイダは暗号化された各ブロック毎にユーザが復号できるか復号できないかを選択する．それらの組合せがユーザのID情報となる．KIK-CDSと提案する配信システムの相違点は，埋め込まれるユーザのID情報が符号化されているか否かである．結託攻撃の種類についてはいくつか考えられるが，本考察では複数の正当なコンテンツ同士を排他的論理和，あるいは論理和により合成することで不正なコンテンツが作成される場合を考察する．例えば，以下の図4において"1"は復号されるブロックを"0"は復号されないブロックを示している．ユーザAとユーザBが各自のコンテンツを論理和によって加算し，結託コンテンツを作成すると，図4(c)のような結託コンテンツとなる．

このように複数のユーザが結託して不正なコンテンツを作り出した時に，その不正なコンテンツから

図 2: 評価用コンテンツ

図 3: 透かし入りコンテンツ

結託したユーザを割り出す方法を以下に示す.

3.2.1 結託者特定アルゴリズム [3]

本手法は通信ネットワークにおける多重化パケットの分離アルゴリズムとして提案されている手法を応用したものである [4]. 透かし情報として埋め込まれているユーザ情報は, ユーザ i の ID 情報として生成多項式 $G_i(x) = g_0(x)G(x)/g_i(x)$ を用いることとする. ここで $g_0(x)$ は全てのユーザの生成多項式に含まれている因数, $g_i(x)(i = 1, 2, \cdots, T)$ は r 次の異なる既約多項式, $G(x) = \Pi_{i=1}^{T} g_i(x)$ とする. T はユーザの人数である. また, $g_0(x)$ と $g_i(x)$ は互いに素である. 符号化, および結託ユーザを特定する手順は以下のようである.

(i) 符号化ユーザ ID $f_i(x)$ は生成多項式 $G_i(x)$ に対応する.

$$f_i(x) = G_i(x) \tag{1}$$

符号化ユーザ ID $f_i(x)$ は, 透かし情報としてコンテンツに埋め込まれる.

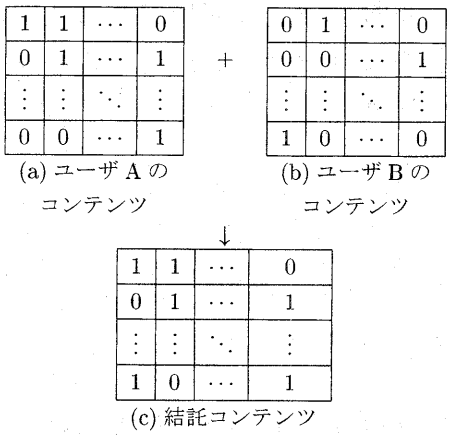

図 4: 結託コンテンツ

(ii) 結託ユーザの ID $f_i(x)$ を論理和や排他的論理和で演算した結託 ID 情報を $F(x)$ とする. $F(x)$ に含まれる誤りを $g_0(x)$ により誤り訂正し, 復号結果を $F'(x)$ とする. [5]

(iii) $F'(x)$ から各ユーザごとの既約多項式を法多項式として剰余 $R_i(x)$ を次式のように求める.

$$R_i(x) \equiv F'(x) \mod g_i(x)(i = 1, 2, \cdots, T) \tag{2}$$

零でない $R_i(x)$ は符号化ユーザ ID $f_i(x)$ に対応しており結託者が特定される.

これにより, 結託コンテンツがユーザの ID 情報の排他的論理和で作成されている場合は結託ユーザを割り出すことが可能である. しかし, 結託コンテンツがユーザの ID 情報の論理和で作成されている場合は 手順 (ii) で誤り訂正する際に訂正能力を超える誤りがあった場合には結託者を割り出せない場合が生ずる.

3.3 提案するコンテンツ配信システムの特徴

提案するコンテンツ配信システムでは, 透かし情報入りコンテンツに復号するための復号鍵そのものに符号化されたユーザ ID 情報が埋め込まれていると考えることができるので, 埋め込まれるべきユーザ ID 情報を改ざんすることは困難であると共に,

プロバイダが送信する情報量が少なくてすむ．また，復号過程でID送付鍵からユーザID情報を分離する必要がないので，ユーザID情報や透かし情報入りコンテンツはデコーダ内で生成されない．そのためユーザによる不正コピーなどの不正行為を抑止可能である．また，ユーザID情報をそのままコンテンツ内に埋め込むのではなく，ユーザID情報を符号化し埋め込むので複数のユーザによる結託攻撃に対しても，不正行為を行ったユーザを追跡し，ある程度特定可能であると考えられる．しかし，3.2.1で述べたように手順(ii)において，結託攻撃が行われても誤り訂正能力を超えないようにパラメータを選択する必要があると考えられる．

4 データ分散共有型ファイル交換システム

4.1 データ分散共有型ファイル交換システムの分類[6]

以下に現在用いられているデータ分散共有型ファイル交換システムを示す．

(i) Server and Client 方式
認証を受けたユーザからの要求に応じて，蓄積されたサーバ内に蓄積されたデータを配信するシステム．

(ii) Hybrid - Peer to Peer 方式
ユーザの経路情報のみをサーバに保管しておき，新たなユーザがシステムに参加する際に，経路情報を配信するシステム．Napstar [7] はこの方式に分類される．

(iii) Pure - Peer to Peer 方式
それぞれのユーザ自身が保管するデータのインデックスをリレー方式でネットワーク内に伝播させていき，要求に応じてユーザが配信するシステム．Gnutella [8] や Freenet [9] はこの方式に分類される．

上記の方式 (i) では，データおよびファイル管理をサーバに集中させるため，データの著作権管理は比較的容易である．しかし，サーバにアクセスが集中した場合高負荷がかかるなどのボトルネックがある．また，(ii) や (iii) の方式ではユーザー間のデータの譲渡に対しデータ著作権の管理はされていない．そこで，本考察では3で提案したコンテンツ配信システムを用い，コンテンツの製作者をシステムに介入させることにより，ユーザ間のデータの譲渡を許しつつ，コンテンツの著作権管理が可能なデータ分散共有型ファイル交換システムの構築が可能となることを示す．

4.2 提案システム

コンテンツのダウンロード要求者をユーザA，コンテンツ共有者をユーザBとする．以下にユーザAがユーザBからコンテンツをダウンロードし，ユーザAの個人情報の入ったコンテンツを得るまでの手順を示す．

step 1 ユーザAはインデックスサーバに対し，コンテンツの検索を行う．

step 2 インデックスサーバはユーザAに対し，検索結果を知らせる．コンテンツの製作会社とユーザBに対し，ダウンロード要求があったことを知らせ，ユーザAとユーザBの接続を確立する

step 3 ユーザAはユーザBからコンテンツをダウンロードする．但し，ダウンロードするコンテンツはユーザBの個人情報が含まれていない評価用コンテンツである．

step 4 ユーザAはコンテンツ使用料を払い，インデックスサーバよりユーザA自身のコンテンツ復号鍵を入手する．

step 5 ユーザAは入手したコンテンツ復号鍵を用いてコンテンツを復号し，ユーザAのユーザ情報の入ったコンテンツを得る．

このようにユーザ間のデータ譲渡を許しつつ著作権管理が可能な，データ分散共有型ファイル交換システムが構築可能となる．

図5に提案方式のブロック図を示す．

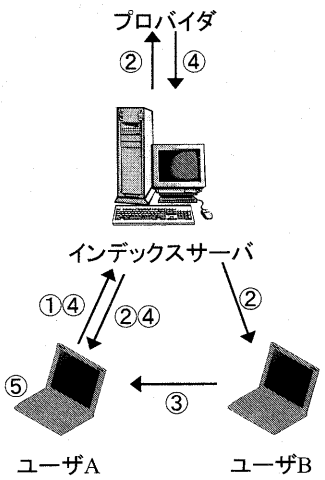

図 5: 提案システム

4.3 提案システムの特徴

提案システムは 4.1(ii) で述べた Hybrid - Peer to Peer 方式を基に構築している．ユーザ間のデータ譲渡を個人情報の含まれない評価用コンテンツで行い，その評価用コンテンツとプロバイダから送られてくるダウンロード要求者自身のコンテンツ復号鍵を用いることでダウンロード要求者は自分自身の個人情報の入ったコンテンツを得る．このことにより，ユーザ間のデータ譲渡を許しつつ著作権管理が可能となる．しかし，データ譲渡を評価用コンテンツで行うので，コンテンツ共有者は評価用コンテンツと自分自身の個人情報の入ったコンテンツの両方を所持する必要があるなどの問題点がある．

5 むすび

本考察では従来のコンテンツ配信システムではあまり検討されていなかった複数のユーザの結託による不正行為について検討を行った．結託攻撃により作成された不正なコンテンツから，電子透かしとして埋め込まれたユーザ ID 情報を利用して結託者を特定する手法について提案を行った．また，提案システムを用いることにより，ユーザ間のデータ譲渡を許しつつ著作権管理が可能なデータ分散共有型ファイル交換システムの構築が可能となることを示した．今後の課題として，提案コンテンツ配信システムにおいては，本考察で取り上げた以外の結託攻撃への対応などが挙げられる．また，データ分散共有型ファイル交換システムにおいては共有者が評価用と自分自身の個人情報の入った両方のコンテンツを所有する必要があるため，ユーザが所有するデータ量が多いなどの問題点が挙げられる．なお，本研究の一部は日本学術振興会科学研究費補助金基盤研究 B(1) 124501571 による

参考文献

[1] 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 (A)，Vol.J82-A No.9 pp.1474-1482(1999).

[2] 角野 英之，稲葉 宏幸，笠原 正雄：" 動画像に適した電子透かしに関する 2，3 の考察"，1998 年暗号と情報セキュリティ・シンポジウム予稿集，SCIS2000-C11(2000).

[3] 蓮尾 知志：" 電子透かしを用いたコンテンツ配信システムの信頼性向上に関する研究"，京都工芸繊維大学卒業研究報告書 (2001)

[4] 秦 淑彦，笠原 正雄，滑川 敏彦:" 代数多重化・多重分離法とそのループネットワークへの応用"，信学論 (B)，Vol.J65-B No.11 pp.1401-1408(1982)

[5] 稲葉宏幸，笠原正雄：" 衝突通信路における符号化パケットの能力に関する二，三の考察"，信学論 (B)，Vol.J75-B-I No.2 pp.99-105(1992)

[6] 石井 陽，稲葉 宏幸：" データ分散音楽配信システムに関する考察"，信学技報，FACE2001，No.11，pp1-6(2001)

[7] Napstar:"Napstar"，http://www.napstar.com

[8] Gnutella："Welcome to Gnutella"，http://welcome.to/gnutella

[9] Freenet："FreenetProject.org"，http://freenetproject.org/cgi-bin/twiki/view/JA/WebHome