論文の内容の要旨

論文題目　Copyright Protection System Using The Fingerprinting Scheme
（フィンガープリンティング方式を用いる著作権保護システム）

氏　名　金 美羅

（本文）情報のデジタル化は，我々の社会や生活に大きな変化と共に新たな問題も引き起こしている．デジタルカメラ，MP3再生機器，PDA，高性能の携帯，大容量ハードディスクを内蔵した再生機器などハードウェアの普及と広帯域インターネットや無線ネットワーク環境の普及は，デジタルコンテンツを楽しめる機会を増やすとともにデジタルコンテンツの配信・交換も活発にさせている．このような環境において，デジタルコンテンツの著作権保護技術は必須になっている．そこで，我々はフィンガープリンティング方式を用いる著作権保護システムに関する考察を行う．

コンテンツのデジタル化が進みにつれて，デジタルコンテンツを不正な二次配布から保護する必要性が高まっている．デジタルコンテンツの編集や複製の容易性，デジタルコンテンツの原本とそのコピーとの区別の難しさ，広帯域インターネットや無線ネットワーク環境の出現などはこのような問題をより深刻にしている．有効な情報を持つユーザにだけコンテンツの取得を許可するアクセス制御機能を提供する暗号技術は一度復号されてコンテンツに対する不正コピーや不正配布に対する保護は不可能である．このような場面で役に立つ技術はフィンガープリンティング (Fingerprinting) である．この技術は，ユーザ ID をデジタルコンテンツの埋め込み情報として利用するため不正配布された不正コピーから不正者の ID を追跡することができる．しかしながら，同じデジタルコンテンツに互い異なるユーザIDを埋め込むため，複数のコピーを入手した不正者はこれらを比較し異なる値を持つ位置を改ざんすることで埋め込まれているユーザ ID をマスクすることができる．これがフィンガープリンティングにおける有効な攻撃として知られている結託攻撃 (Collusion attack) である．

結託攻撃の対策として，ユーザ ID を結託に耐性を持つ符号 (c-secure code) で符号化する思想が提案されている．c-secure 符号は，最大 c 人の結託者グループに対して少なくとも一人を不正者として特定することができる．c-secure 符号はユーザ ID の数と結託参加人数が増えると符号長が急激に増えてしまうため，実際応用には難しい．そこで，我々は結託に耐性を持つと共に短い符号を構成するため，有限体上の度数多項式環の剰余環における中国人剰余定理を利用する c-secure CRT 符号の構成方式を提案し，従来方式と提案方式との性能を比較する．

一方，不正者追跡のため異なるユーザ ID をデジタルコンテンツに埋め込むため，これらのコンテンツの配布を考慮しなければならない．このような問題の直観的な解決策として Broadcast Encryption が考えられる． Broadcast Encryption とは，センターが送信した暗号化データに対して，有効な(i.e. 復号)鍵を持つ受信者 (privileged users) のみがそのデータを復号できる方式である．このような方式は，pay-TV system, multicast communication, CD/DVD などを用いた著作物の配布などに有用である．しかしながら，Broadcast Encryption のみではコンテンツの暗号化および再生機器内の鍵の漏洩に対処できても，復号されたコンテンツの不正な二次配布には対処できない．そ

れは，Broadcast Encryption では同一のデータを受信者に送信するため，送信者側でコンテンツに受信者ごとに異なる電子透かしを埋め込むことは難しい．このための解決策として，受信者の再生機器に透かしの埋め込みアルゴリズムを内蔵してコンテンツが再生される際に fingerprint を埋め込むことも可能であるが，この場合再生機器が解析され透かしの埋め込みアルゴリズムが暴かれ，透かしを消去するプログラムが作成・配布される危険性がある．そこで，我々は透かしの埋め込みアルゴリズムを再生機器に入れることなく fingerprint を埋め込む方式を提案し，それを効率よく実現するために，およそ半分の受信者を効率よく無効化できる Broadcast Encryption 方式を提案する．提案方式は，フィンガープリントの埋め込みは勿論，番組の視聴者数が許容視聴者数の半数程度しかいない放送番組の暗号化にも向いている．

さらに，ソフトウェア保護のための技術の一つであるソフトウェア電子透かしの安全性に対する考察を行っている．