様式 C-19

科学研究費補助金研究成果報告書

平成　２１年　６月　２日現在

研究種目：若手研究（Ｂ）
研究期間：2007 年～2008 年
課題番号：19760254
研究課題名（和文）　ディジタルコンテンツの著作権保護のための電子的な指紋生成及び管理技術
研究課題名（英文）　Digital fingerprinting system for the protection of the ownership of digital contents

研究代表者
栗林　稔　(KURIBAYASHI MINORU)
神戸大学・大学院工学研究科・助教
研究者番号：50346235

研究成果の概要：
本研究では，スペクトル拡散技術に基づく電子指紋技術において，ディジタル画像を通信路と見立てて，埋め込む指紋信号を送受信するデータにモデル化し，通信路の周波数帯域を複数のユーザで共有できる CDMA 技術を導入した．本システムでの指紋信号は，直交系列である DCT 基底ベクトルを特定の PN 系列で変調させている．指紋信号を 2 成分に分けて更に PN 系列の特性を利用して階層構造を与えることで，結託者の特定に要する計算量を従来法に比べて大幅に削減させた．この階層構造を与える手法を結託耐性符号の構成にも応用させて，従来では難しかった実時間内での検出を可能とさせた．結託人数の増加に伴い指紋信号間の干渉成分が増大するが，これらを理論的に考察し，効率良く干渉成分を削減する手法を提案した．その結果，従来手法に比べて結託耐性を向上させることに成功し，要する計算量を対数オーダーで削減できることが確認された．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	2,000,000	0	2,000,000
2008 年度	1,200,000	360,000	1,560,000
年度			
年度			
年度			
総　計	3,200,000	360,000	3,560,000

研究分野：　工学
科研費の分科・細目：　電気電子工学・通信・ネットワーク工学
キーワード：電子指紋技術，結託攻撃，CDMA 技術，結託耐性符号

１．研究開始当初の背景

ディジタルコンテンツの不正コピーの蔓延を防ぐ技術として電子指紋技術が考案されている．この技術を用いた電子指紋システムにおいて，深刻な問題が結託攻撃である．なぜならば，購入者ごとに僅かに異なる信号を密かに埋め込んだコンテンツを配信しているため，複数持ち寄ればその違いを調べて指紋信号を改変もしくは除去される恐れがあるからである．従来は複数の不正者による結託攻撃を考慮して，ある程度までの結託であれば耐性のある特殊な符号（結託耐性符号）を効率良く構成する研究がなされていた．また，ユーザごとに異なる復号デバイスや復

号鍵を与えることにより，これらが流出した場合に追跡できる不正者追跡方式の研究がなされていた．実際の埋め込みを考慮した手法としては，スペクトル拡散技術を用いる方式が提案されていたが，検出に要する計算量が非常に大きいため，近年では電子指紋符号の方にその研究の主流が傾いていた．

２．研究の目的

電子指紋システムにおいて，結託攻撃に対するアプローチとしてスペクトル拡散技術に着目し，結託耐性符号と同等もしくはそれ以上の不正者追跡能力を有する手法を考案する．DVD に収めされる映像だけでなく，静止画像においても適用できるほどの効率を追及する．また，特定のコンテンツに限定せず，ディジタルコンテンツであればすべてにおいて適用できるように汎用性を兼ね備えた方式を考案する．結託攻撃だけでなく電子透かし方式の評価に用いられる攻撃との複合的な処理に対しても耐性を有する方式を構築し，その不正者の検出能力を評価する．特に，誤って無実のユーザを不正者として検挙する誤検出率をシステムに応じて設定できるように理論的に解析し，実証実験を行う．更には，その設定値において最適な不正者の検挙ができるシステムの構築を目指す．

３．研究の方法

本研究では，擬似直交系列を用いてコンテンツに仮想的に直交する情報を埋め込む技術を発展させることにより実用的な構成法を研究する．現在構想を得ている手法は，CDMA に代表される通信路の多重化技術を応用させる方法である．一つの通信路を複数のユーザで共有させて使用することができる多重化技術において，通信路をコンテンツとみなし，利用者が送信する情報を電子指紋情報とみなせば，コンテンツ配信サービスにおける不正者追跡システムに応用させることができる．擬似直交系列を用いて符号分割する CDMA のように，電子指紋情報を巧妙に符号化させれば，符号長を短く抑えつつ結託攻撃に耐性を持たせることが可能である．

スペクトル成分の統計的な分布がガウス分布に理論的に近似できる．また，埋め込みの際に用いる秘密鍵が分からなければ，攻撃者がコンテンツから電子指紋情報を取り除くもしくは改変させる処理（例えば，各種フィルタリング，雑音付加や非可逆圧縮）により生じるスペクトル成分への影響もまたガウス分布に理論的に近似できる．そこで，確率モデルに基づくシステム設計を行うために，まず各パラメータに対する理論値を推定し，計算機シミュレーションにより実証実験を行う．

電子的な指紋の埋め込みによるシステムで最も重要なことは，非対称性の実現である．非対称性とは，コンテンツの売買プロトコル終了後には，購入者だけが電子指紋の埋め込まれたコンテンツを得られる特性である．もし，販売者もそのコンテンツを持つならば，たとえ不正コピーを発見してその電子指紋が検出されたとしても，購入者の不正を法的に立証できない．なぜならば，販売者自身が購入者を陥れるためにコンテンツを流す恐れがあるからである．そこで，上記の電子指紋の埋め込み処理を単純に行うのではなく，暗号化された領域での処理ができるように修正する．その際，公開鍵暗号の準同型写像の性質を用いる手法に適用する．

４．研究成果

電子指紋システムの構築のために，まず電子指紋信号を次のように作成した．直交系列である DCT 基底ベクトルに，擬似直交系列である PN 系列を乗算してスペクトル拡散系列を作成する．許容ユーザ数の拡大を目的として，ユーザを特定する情報を，グループ ID とユーザ ID の二種類の ID 情報で構成し，グループ ID に対応するスペクトル拡散系列を割り当て，そのグループ ID に基づいて作成したユーザ ID 用のスペクトル拡散系列を割り当てる．これらの二種類のスペクトル拡散系列を多重化させてコンテンツの特定の周波数成分に加算して埋め込みを行う．これらの系列は互いに擬似直交するため，その干渉は低く抑えられる．それゆえ，検出の際にはまずグループ ID を検出し，それに対応するユーザ ID の検出を試みるように 2 段階の操作を行う．

この 2 段階の操作の特徴を利用して，干渉成分をさらに抑える手法を提案した．グループ ID を検出した後で，検出された信号成分を干渉成分として除去することで，ユーザ ID の検出精度の向上を図った．この処理は繰り返し行うことが可能であり，繰り返す度に干渉成分が除去され，雑音や干渉成分に埋もれていた信号も，効果的に検出できる方式を実現させた．評価として，512×512 画素，白黒濃淡 256 階調の標準画像”lena”を用いて実験を行った結果を図 1 に示す．ただし，

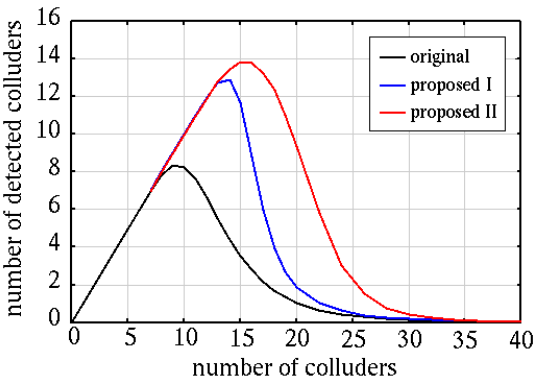

図 1　検出された不正者の数

original は干渉除去なし，proposed I は干渉除去有り，proposed II は干渉除去を繰り返したものである．また，系列長は 1024，許容ユーザ数は 100 万人であり，攻撃として平均化攻撃と品質 35%の JPEG 圧縮を施した．図 2 は，系列長を変化させた場合の結果である．干渉成分を除去しない場合と比べて，干渉成

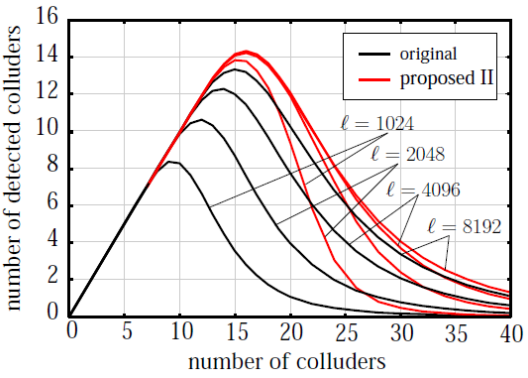

図 2　異なる系列長において，
検出された不正者の数の比較

分を除去することにより，検出できる結託者の人数は飛躍的に上昇できることがこれらの結果より確認された．　また，閾値の設定には，統計的な手法を用いて誤検出率に応じて計算することで，検出率は向上させつつ誤検知率の削減を図っている．その誤検出率を表 1 にまとめている．

表 1　誤検出率[$\times 10^{-4}$]

系列長	original	proposed I	proposed II
1024	2.00	2.63	3.04
2048	2.08	3.08	1.08
4096	1.54	3.17	1.08
8192	3.83	4.38	1.58

提案手法の主な利点は，その検出に要する計算量である．従来方式では，候補となるスペクトル拡散系列すべてと相関計算をする必要があったため，1 回の検出に要する計算量は符号長を L，許容ユーザ数を N とすると，$O(NL^2)$ であった．提案手法では，検出の際に行う DCT 変換には高速アルゴリズムを利用でき，さらに階層構造による 2 段階の検出操作のため，その計算量は $O(c\sqrt{NL}\log L)$ となる．干渉除去の際に繰り返し処理をしたとしても，従来手法と比べてはるかに少ない計算量で検出できる．図 4 は実際に PC 上で測定した時間である．ただし，実装環境は，CPU に Core2Quad Q6700 (2.66GHz)，メモリ 8GB，OS は CentOS 5.1 X86_64 バージョンである．

非対称電子指紋プロトコルにおいて，スペクトル拡散技術に基づく電子指紋方式を適

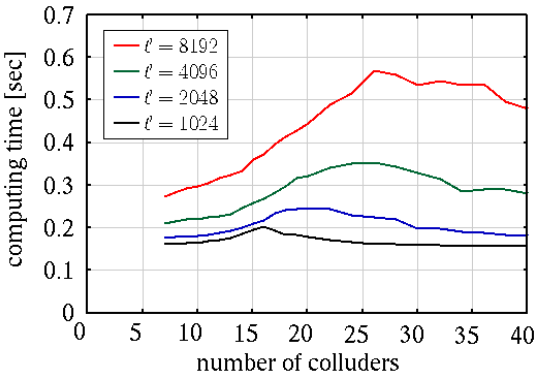

図 4　計算時間の評価

用させるため，暗号プロトコルに実装できるようにプロトコルを修正した．その際に問題となることは，量子化による精度の低下と，送信すべきデータ量の増加である．これらの問題を解決すべく，スケーリングパラメータとパッキン処理を提案し，実装評価を行った．その結果，従来方式と比べて暗号化率を 1/50 程度に抑えることに成功し，その時の結託耐性はほとんど劣化しないことを確認した．

以上の結果をまとめれば，法的に不正者の検挙が可能であり，結託耐性を有する電子指紋システムの構築が行えたと結論付けられる．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　9 件）

① M. Kuribayashi and M. Morii, "A study on the traceability of CDMA-based fingerprinting scheme," The 2009 Symp. on Cryptography and Information Security, Jan. 2009.

① M. Kuribayashi and M. Morii, "Iterative detection method for CDMA-based fingerprinting scheme," IH'08, LNCS 5284, pp. 357-371, Springer-Verlag, 2008. （査読有）

② M. Kuribayashi and M. Morii, "Effective detection method for CDMA-based fingerprinting scheme," 2008 IEEE Int. Conf. Multimedia & Expo (ICME2008), pp. 349-352, 2008. （査読有）

③ M. Kuribayashi and M. Morii, "On the implementation of asymmetric fingerprinting protocol," 16th

European Signal Processing Conference (EUSIPCO2008), SS7-1, 2008. (査読有)

④ M. Kuribayashi, N. Akashi, and M. Morii, "On the systematic generation of Tardos's fingerprinting codes," IEEE Signal Processing Society, 2008 Int. Workshop on Multimedia Signal Processing (MMSP2008), pp.748-753, 2008. (査読有)

⑤ N. Akashi, M. Kuribayashi, and M. Morii, "Hierarchical construction of Tardos code," 2008 International Symposium on Information Theory and its Applications (ISITA2008), pp.683-688, 2008. (査読有)

⑥ H. Kato, M. Kuribayashi, and M. Morii, "Effective assignment of fingerprints on CDMA-based fingerprinting scheme," 2008 International Symposium on Information Theory and its Applications (ISITA2008), pp.694-699, 2008. (査読有)

⑦ H. Sakai, M. Kuribayashi, and M. Morii, "Adaptive reversible data hiding for JPEG images," 2008 International Symposium on Information Theory and its Applications (ISITA2008), pp.870-875, 2008. (査読有)

⑧ 田中敏也, 栗林稔, 森井昌克, "一方向性関数を用いた任意の有効期間設定が可能な時限付き鍵管理技術," 情報処理学会論文誌, vol.48, no.9, pp.3089-3098, 2007.(査読有)

⑨ N. Hayashi, M. Kuribayashi, and M. Morii, "Collusion-Resistant Fingerprinting Scheme Based on the CDMA-Technique," IWSEC2007, LNCS 4752, pp.28-43, Springer-Verlag, 2007. (査読有)

〔学会発表〕(計 9件)

① M. Kuribayashi and M. Morii, "A study on the traceability of CDMA-based fingerprinting scheme," The 2009 Symp. on Cryptography and Information Security, Shiga, Japan, Jan. 20-23, 2009.

② 明石直之, 栗林稔, 森井昌克, "Tardos符号のトレーサビリティの評価," 2008年暗号と情報セキュリティシンポジウム, 2008年1月22日～25日. ファニックスシーガイアリゾート.

③ 加藤寛史, 林直樹, 栗林稔, 森井昌克, "CDMA技術に基づく電子指紋方式の階層構造の拡大," 2008年暗号と情報セキュリティシンポジウム, 2008年1月2日～25日. ファニックスシーガイアリゾート.

④ M. Kuribayashi and M. Morii, "On the performance analysis of detection method for CDMA-based fingerprinting scheme," The 2008 Symp. on Cryptography and Information Security, 22-25, Jan, 2008. Miyazaki, Japan.

⑤ 門田宜也, 栗林稔, 森井昌克, "計算量の観点による2階層Tardos符号の最適化," コンピュータセキュリティシンポジウム2008, 2008年10月8日～10日. 沖縄コンベンションセンター.

⑥ 山根進也, 栗林稔, 森井昌克, "非対称電子指紋プロトコルの実装について," 電子情報通信学会 ISEC研究会, 2007年9月7日. 機械振興会館.

⑦ 林直樹, 栗林稔, 森井昌克, "CDMA技術に基づく電子指紋方式のスペクトル系列構成法の検討," 第30回情報理論とその応用シンポジウム, 2007年11月27日～30日. 賢島宝生苑.

⑧ M. Kuribayashi, N. Hayashi, M. Morii, "Effective detection method for CDMA-based fingerprinting scheme," The 30th Symp. on Information Theory and its Applications, Kashikojima, Mie, Japan, Nov. 27-30, 2007.

⑨ 酒井宏誌, 栗林稔, 森井昌克, "JPEG圧縮における可逆データハイディング," 第30回情報理論とその応用シンポジウム, 2007年11月27日～30日. 賢島宝生苑.

６．研究組織

(1)研究代表者

栗林 稔 (MINORU KURIBAYASHI)
神戸大学・大学院工学研究科・助教
研究者番号：50346235