様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月 ２６ 日現在

機関番号：１４５０１
研究種目：若手研究(B)
研究期間：2012～2014
課題番号：２４７６０２９９

研究課題名（和文）実用的な不正コピー管理システム

研究課題名（英文）Practical Managemet System for Multimedia Content

研究代表者
栗林　稔（KURIBAYASHI, MINORU）

神戸大学・工学（系）研究科（研究院）・助教

研究者番号：５０３４６２３５

交付決定額（研究期間全体）：（直接経費）　　3,300,000円

研究成果の概要（和文）：海賊版コピーから不正に関わったユーザを特定するための電子指紋技術において，スペクトル拡散技術に代表される信号処理技術を用いて，計算量を抑えつつ多くの不正者を特定できる検出器を開発した．誤って無実のユーザを検挙してしまう冤罪確率を極めて低く抑えつつ，多くの不正者を特定することに成功した．また，結託耐性符号においては，不正者に有利な攻撃仮定において，最適な検出器の設計を行った．しかし，不正者の人数や攻撃方法の情報を予め入手する必要があり，事実上実現は困難であった．そこで，統計的な解析と近似処理によりこれらの情報を必要とせず，最適な検出器と極めて近い性能を示す検出器の実現に成功した．

研究成果の概要（英文）：Fingerprinting technique enables us to identify illegal users from a pirated copy of multimedia content. In this study, I developed an efficient detector based on signal processing techniques involving a spread spectrum method. Even if more than 100 illegal users collude, the proposed detector can detect almost all of them with reasonable computational costs. The probability that innocent users are accused by chance is limited to be extremely small. I also developed an optimal detection algorithm for a collusion secure code under a realistic threat of collusion attack. Since the optimal algorithm requires the number of illegal users and their attack straregy in advance, it is difficult to realize in essense. In order to make it practical, I introduced a statistical analysis and approximations at the detection algorithm. As the results, I succeedded to realize a simplified detection algorithm which performance is remarkably close to the optimal one.

研究分野：情報セキュリティ

キーワード：電子指紋技術　スペクトル拡散　電子透かし　結託耐性符号

１．研究開始当初の背景
ブロードバンドネットワーク環境の普及により，著作物の権利侵害行為にも多様性が生じており，その取締りは益々困難なものとなっている．IT 技術に関連する最新技術には利便性の追求が優先される傾向があり，セキュリティに関する考察が不十分なために，悪意を持った個人や団体が恣意的に技術を利用するケースが多々見受けられる．ネットワークストリーミング配信として，YouTube や Ustream などのように個人が自由にコンテンツを配信できるサービスは利用者側に恩恵をもたらしているが，深刻な著作権侵害問題が発生している．投稿されるコンテンツには，TV 放送を録画したものから，DVD から抜き出した動画，音楽ファイルなど多種多様にわたっており，現在のところ著作権保有者もしくはその代理人による申し立てを受けて削除する対策がなされている．このような対策を自動に処理できる技術の開発は，今後のコンテンツビジネスを展開していく上で，必要不可欠なものである．

最近では，DRM(Digital Right Management)技術によりコンテンツ保護を目指しているが，主にデータをメディアから抽出させることを防ぐ方法である．また，B-CAS では正規ユーザ以外はスクランブル化されたコンテンツを復号できないようにする処理がなされるだけである．そのため，正規ユーザがコンテンツを入手した後に海賊版コピーを流通させる可能性は排除できない．

２．研究の目的
電子著作物の権利保護を目的として，海賊版のデータを不正に流出させた不正者を検挙するために電子的な指紋情報を生成し，海賊版のデータから効率良く不正者を検挙できるシステムの構築を行う．また，どのような攻撃環境においても，無実のユーザを誤って検挙する冤罪を極めて低く抑えつつ，高速に動作する検出器の開発を行う．

スペクトル拡散技術に基づく電子指紋方式と結託耐性符号の研究において，結託攻撃に対する解析は特定の理想的な攻撃モデルの状況下でなされており，実際になされる海賊版のコピーの作成環境とは乖離したものであった．本研究では，実環境になるべく近い攻撃モデルにおいて，従来の手法がどの程度の効果を発揮するのかを理論的な解析と計算機シミュレーションを通して調べる．また，冤罪確率を低く設定しつつ，検出できる不正者の数を増やすことのできる検出手法の開発だけでなく，符号構成における考察も併せて行う．

３．研究の方法
ディジタルコンテンツを受信する利用者ごとに僅かに異なる情報を埋め込む電子指紋システム上で最も深刻な問題は，利用者の結託である．単純に異なる情報を埋め込む場合，利用者がお互いのコンテンツを比較することにより埋め込まれている情報を改変もしくは除去する恐れがある．

スペクトル拡散技術に基づく方式では，符号間干渉成分の除去と繰り返し検出によって検出精度を高められることが知られている．従来手法は，少ないユーザ数において適用できるが，本研究で想定している結託者数の場合，その組み合わせの数が莫大であるため，全パターンを探索することは計算量的に極めて困難である．そこで本研究では，新規アイディアとして最初のループで検出される信号の組み合わせを考慮して符号間干渉成分の除去を行い，続くループで検出される信号を追加した組み合わせで更なる除去処理を行うように，逐次的に部分最適化処理を解く手法を着想している．このアイディアに基づいて電子指紋信号の適応的な検出処理の理論的な能力解析と計算機による評価を行う．

また，同時並列として結託耐性符号として最近注目を集めている Tardos 符号とその関連符号において，実環境を想定した攻撃モデルと運用モデルでの性能評価を行い，最適な検出方法の理論的な導出と実証実験を行う．従来行われてきた結託耐性符号の性能評価は，マーキング仮定と呼ばれる攻撃モデルであり，現実に起こり得る攻撃とは乖離していた．このモデルでは，雑音付加などの符号語に生じる歪みが考慮されていなかった．本研究では，ガウス雑音だけではなくコンテンツへの攻撃によって生じる可能性のある雑音成分を考慮して，検出器において雑音モデルを検知させ，その雑音の特徴に応じた最適な検出器を構築する．そのためには，最大事後確率を求め，攻撃パターンに応じた重み付けをした検出アルゴリズムが不可欠である．実用的に検出器を設計するためには，これらの操作が不可欠であり，これらを理論的な観点からのアプローチとヒューリステックな方法によるアプローチの両方を並列して行う．

４．研究成果
スペクトル拡散技術に基づく方式では，直交系列である DCT 基底ベクトルに拡散系列を乗算して作成したスペクトル拡散系列を各ユーザに割り当てる手法を提案した．この手法では，複数のユーザをグループごとに検出できる階層化構造をしていることから，検出に要する計算量を対数オーダーに抑えることができる．また，高速 DCT アルゴリズムの適用によって更に計算量を削減できる．それ故，通常の検出であれば数十ミリ秒程度で実行することが可能となった．

この検出器において，1 回目の検出の際に誤り検出をある程度許容する形で，なるべく疑わしい信号を多く検出する方針を取る．続いて，検出された信号を干渉成分とみなして除去してから，2 回目の検出を行うことにより 1 回目では干渉成分により埋もれていた信号まで検出可能となる．この操作は，これ以上信号の検出ができなくなるまで繰り返し行うことで，検出性能の向上に成功した．

図 1 は，ユーザ数が約 100(=2^{20})万人のシステムにおいて，512×512 画素のカラー画像 lena に長さ 4096 の電子指紋信号を埋め込み，複数の不正者により作成された海賊版コピーから特定できる不正者の人数を示している．ただし，海賊版のコピーは，非可逆圧縮である JPEG アルゴリズムで二次攻撃が加えられている．

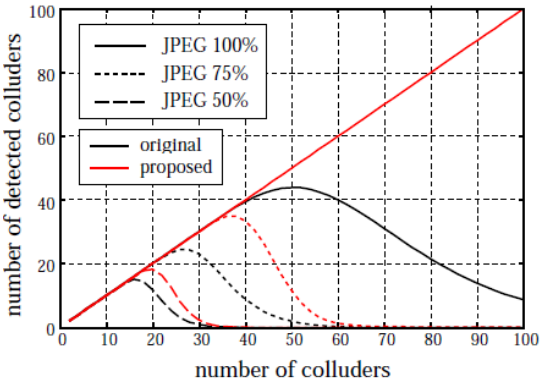

図 1．検出性能の比較

図に示す JPEG のパーセンテージは圧縮品質(quality factor: QF)である．この図より，提案した繰り返し干渉成分除去方式は通常の検出器に比べて，その性能を飛躍的に高めていることが分かる．特に，二次攻撃が加えられていなければ，100 人が結託しても，海賊版コピーより全員を特定することが可能となっている．

次に QF=75%において他の画像に対して性能評価を行った結果を図 2 に示している．画像によって生じた検出性能の差は，主に二次攻撃である JPEG 圧縮に依るものである．

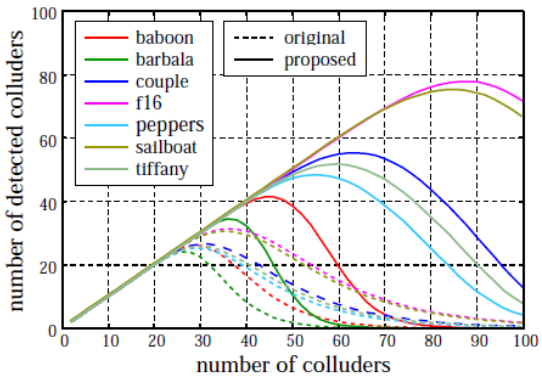

図 2．画像ごとの検出性能の違い

図 3 は，検出時間を示している．ただし，CPU は Intel Core i7 860，RAM メモリは 8GB の PC で測定した結果であり，画像の読み込みなどで 0.1 秒ほど要している．この結果から，不正ユーザが 100 人においても 0.6 秒弱で検出できることが分かり，提案検出器は極めて実用的であることが分かる．

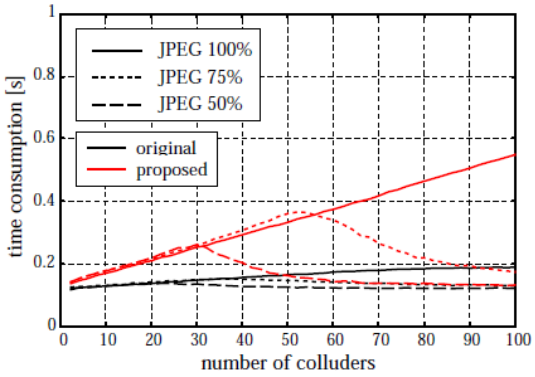

図 3 計算時間の評価

なお，計算機シミュレーションを通して，誤って無実のユーザを検挙する冤罪確率は 10^{-4} で設定しており，実際のデータにおいてもこの確率を下回ることを確認している．

結託耐性符号の研究においては，マルチメディアコンテンツに埋め込んで利用する環境を想定し，攻撃モデルを再評価した．その結果，従来のマーキング仮定に基づく攻撃だけでなく，雑音付加も考慮する必要があることを示した．また，信号処理空間における攻撃と，符号語空間における攻撃を想定する必要があり，従来に比べてより煩雑な解析が不可避であることも示した．一方，符号語空間への直接的な攻撃を防ぐことができれば，マーキング仮定による攻撃モデルよりも，攻撃者にとって不利となる環境を与えられることも解析により明らかにした．

符号語空間へのアクセスを防ぐ目的で，スペクトル拡散に基づく電子指紋方式に着目し，OFDM 通信のような変調を信号処理空間で与える方式を提案した．その方式では，符号語の各ビットが広範囲の周波数成分に拡散された形にしており，拡散系列の秘匿性を根拠に直接的なビットの改変を困難とした．その結果，最悪の攻撃シナリオが信号レベルを減衰させる平均化攻撃となるようにシステムを構築することに成功した．提案システムでは，マルチメディアコンテンツに付加される雑音が，符号語を検出する信号領域においてガウス雑音にモデル化できる利点もあることをシミュレーションにて確認している．

続いて，平均化攻撃とガウス雑音付加の環境において最適な(MAP)検出器の設計を行った．残念ながら MAP 検出器では，前もって不正ユーザの人数が必要であり，計算も複雑となり，

更には雑音の量が増えるに従ってその推定が困難となる問題があった．そこで，近似計算をうまく利用することにより，単純な処理だけで最適値と極めて近い検出性能を示す検出器を提案した．

図 4 では，AWGN 通信路を仮定して提案検出器が最適な MAP 検出器との性能を比較した結果である．この図から，SNR があまり大きくない環境では，提案検出器は最適な検出器と同程度の性能を示すことが分かる．

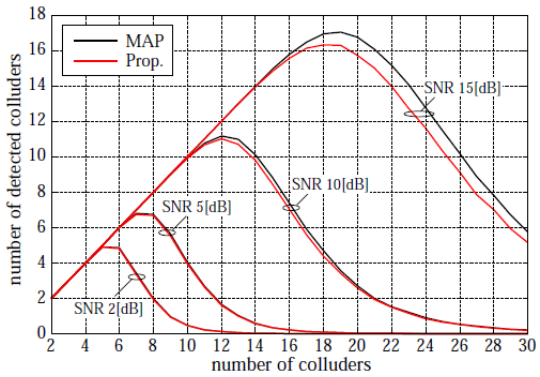

図 4 結託耐性符号における最適な検出器との検出性能の比較

次に，カラー画像に対して電子指紋符号を埋め込んで，結託攻撃により作成した海賊版コピーから不正ユーザの検出を試みた．実環境を想定して，符号語を埋め込んだ画像は，まず 1 回目の JPEG 圧縮を行い，複数の JPEG 画像を平均化した後に，2 回目の JPEG 圧縮を行う実験を行った．この環境は，起こり得るコンテンツの流通経路を想定したものである．その結果，符号語を検出する信号領域において，加法性白色ガウス雑音が付加されるだけでなく，信号が減衰することが判明した．そこで，最適な検出器においては更なる推定器が必要となることから，実環境において実現は更に困難であることが分かった．一方提案検出器では，極めて簡単な処理を追加するだけで対応可能であり，実用的な方式であることを改めて示すことができた．

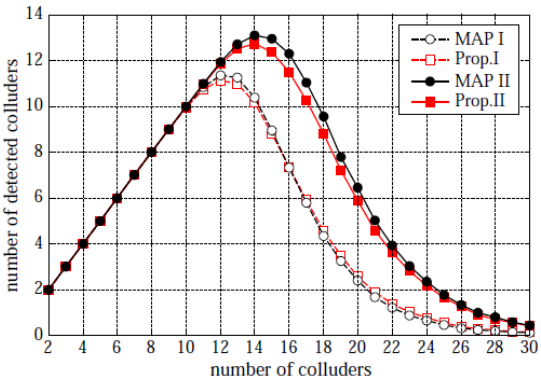

図 5 実環境における性能比較

図 5 では，画像 lena に対して符号語を埋め込み，1 回目は QF=75%，2 回目は QF=50%として JPEG 圧縮を行って作成した海賊版コピーから検出された不正ユーザ数を示している．ただし，MAPII は MAP(最適な検出器)に不正ユーザ数と減衰係数を既知として与えた比較用の最適値であり，prop.II は信号の減衰を考慮した提案検出器である．この結果より，提案検出器は実環境においても最適値に極めて近い特性を持つことが示された．提案検出器は，その実装も比較的容易であり少ない計算量で実現できることから，実用的な方式であることが示された．

開発した電子指紋システムは動画像に適用することも可能である．リアルタイム処理までは難しいが，従来の方式に比べて飛躍的に実用性を高めることができることを上述の研究成果より確認することができる．

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　8 件）

① M. Kuribayashi, "Countermeasure to Non-Linear Collusion Attacks on Spread Spectrum Fingerprinting," Proc. ISITA2014, pp.50-54, 2014. 査読有
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=6979801&abstractAccess=no&userType=inst

② M. Hakka, M. Kuribayashi, M. Morii, "DCT-OFDM based watermarking scheme robust against clipping attack," Proc. IWIHC2014, pp.18-24, 2014. 査読有
DOI: 10.1145/2598908.2598914

③ M. Kuribayashi, "Simplified MAP detector for binary fingerprinting code embedded by spread spectrum watermarking scheme," IEEE Trans. Information Forensics and Security, vol.9, no.4, pp.610-623, 2014. 査読有
DOI: 10.1109/TIFS.2014.2305799

④ M. Kuribayashi, "A simple tracing algorithm for binary fingerprinting code under averaging attack," The 1st ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec'13), pp.3-11, 2013. 査読有
DOI: 10.1145/2482513.2482521

⑤ M. Kuribayashi, "Coded spread spectrum watermarking scheme," 11th Int. Workshop on Digital-forensics and Watermarking (IWDW2012), LNCS 7809, Springer-Verlag, pp.169-183,

2013. 査読有
DOI: 10.1007/978-3-642-40099-5_15

⑥ M. Kuribayashi, "Analysis of binary fingerprinting codes under relaxed marking assumption," 2012 Int. Symp. on Information Theory and its Applications (ISITA2012), pp.643-647, 2012. 査読有
http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=6401018&abstractAccess=no&userType=inst

⑦ M. Kuribayashi, "Bias equalizer for binary probabilistic fingerprinting codes," 14th Information Hiding Conference (IH2012) LNCS 7692, Springer-Verlag, pp.269-283, 2012. 査読有
DOI: 10.1007/978-3-642-36373-3_18

⑧ M. Kuribayashi, "Interference removal operation for spread spectrum fingerprinting scheme," IEEE Trans. Information Forensics and Security, vol.7, no.2, pp.403-417, 2012. 査読有
DOI: 10.1109/TIFS.2011.2170421

〔学会発表〕(計 19 件)

① 電子情報通信学会 情報理論研究会 招待講演: 栗林稔, "電子指紋符号の最適な検出法," 信学技法, IT 9 月, 2014. 館山市(千葉県)

② 第 36 回情報理論とその応用シンポジウム(SITA2013)ワークショップ: 栗林稔, "電子指紋符号の研究紹介," 2013 年 11 月. 伊東市(静岡県)

③ 第 26 回回路とシステムワークショップ招待講演: 栗林稔, "学生向け電子透かしチュートリアル," 2013 年 7 月. 淡路夢舞台(兵庫県)

④ M. Kuribayashi, "Estimation of noise channel from fingerprinting codeword," Proc. 2013 IEEE International Workshop on Information Forensics and Security (WIFS2013), Nov. 2013. 広州(中国), 査読有

⑤ M. Kuribayashi, "Study on Collaboration of Collusion Secure Code and Watermarking Technique," Technical Report of IEICE, EMM Jan. 2015. 東北大学(宮城県)

⑥ M. Kuribayashi, "Study on Scoring Function of Binary Fingerprinting Codes," SCIS2015, 2015. 小倉市(福岡県)

⑦ M. Kuribayashi, "Watermarking Security Based on Kerchhoffs' Principle," Technical Report of IEICE, EMM Nov. 2014. 九州大学(福岡県)

⑧ M. Kuribayashi, "Simplified tracing algorithm of fingerprinting code against averaging attack," Technical Report of IEICE, EMM Mar. 2014. 北陸科学技術先端大学(石川県)

⑨ M. Kuribayashi, "Study of the Security on Spread Spectrum Fingerprinting," SCIS2014, 2014. 鹿児島市(鹿児島県)

⑩ M. Kuribayashi, "Estimation of Noisy Channel from Distorted Fingerprinting Codeword," SITA2013, 2013. 伊東市(静岡県)

⑪ 八家匡希, 栗林稔, 森井昌克, "切り抜き攻撃に耐性を持つ DCT-OFDM 型電子透かし方式," 信学技法, EMM 11 月, 2013. 県立広島大学(広島県)

⑫ M. Kuribayashi, "Optimal Tracing Algorithm for Fingerprinting Code under Averaging Attack," Technical Report of IEICE, EMM, May 2013. 高知市(高知県)

⑬ 合志清一, 栗林稔, 竹下寛久, 越前功, 岩田基, 岩村惠市, "第 1 回画像・映像電子透かしコンテスト実施結果とその講評," 信学技法, EMM 1 月, 2013. 東北大学(宮城県)

⑭ 八家匡希, 栗林稔, 森井昌克, "DCT-OFDM に基づく電子透かしの耐性向上," SCIS2013, 2013.京都市(京都府)

⑮ M. Kuribayashi, "Collusion Secure Blind Fingerprinting Scheme," SCIS2013, 2013. 京都市(京都府)

⑯ 合志清一, 栗林稔, 越前功, 岩田基, 川村正樹, 岩村惠市, "画像・映像信号用電子透かし評価基準 2013 の提案," SCIS2013, 2013.京都市(京都府)

⑰ 八家匡希, 栗林稔, 森井昌克, "重み一定符号化したスペクトル拡散型電子透かし," SITA2012, 2012.別府市(大分県)

⑱ M. Kuribayashi and M. Morii, "Coded OFDM system with spreading operation," SITA2012, Dec. 2012. 別

府市(大分県)

⑲ M. Kuribayashi, M. Hakka, and M. Morii, "OFDM-type spread spectrum watermarkging scheme," Technical Report of IEICE, EMM Nov. 2012. 大分大学(大分県)

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)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

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：