様式 C-19

科学研究費補助金研究成果報告書

平成 22 年 5 月 31 日現在

研究種目： 若手研究（B）
研究期間：2008 年度～2009 年度
課題番号：20760249
研究課題名（和文）マルチメディアコンテンツの著作権保護を目的とした高効率なデジタル指紋符号の開発
研究課題名（英文）Development of highly efficient digital fingerprinting codes for multimedia
研究代表者 八木 秀樹（Hideki Yagi）
電気通信大学・先端領域教育研究センター・特任助教
研究者番号：60409737

研究成果の概要（和文）：
デジタル指紋技術は著作権により保護されたデジタルコンテンツが不正に利用された場合に，不正利用者を検出するための技術として注目を集めている．本研究では，画像データや音声データなどのマルチメディアに用いられるデジタル指紋に対し，効率的な符号化法の開発を行った．特に，不正者数がある定数以下の場合に，全ての不正者を検出できるシステムの効率化を行い，少ない計算コストで不正者を検出できる符号化法を提案した．

研究成果の概要（英文）：
Digital fingerprinting is a technique for identifying malicious users when a digital content protected by copyright is illegally used. In this research, digital fingerprinting codes for multimedia were developed. In particular, when the number of malicious users is less than or equal to some pre-determined number, a number of new coding methods were developed so that the efficiency of the fingerprinting codes is improved and the codes can be implemented with low computational complexity.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	500,000 円	150,000 円	650,000 円
2009 年度	500,000 円	150,000 円	650,000 円
総　計	1,000,000 円	300,000 円	1,300,000 円

研究分野：工学
科研費の分科・細目：通信・ネットワーク工学
キーワード：情報セキュリティ，符号化，デジタル指紋，マルチユーザ符号化，多重アクセス通信路，誤り訂正符号，マルチユーザ情報理論

１．研究開始当初の背景

近年，デジタル画像や音楽ファイルなど知的所有権により保護されたデジタルコンテンツが取り扱われる機会が増えている．今日の情報化社会において，デジタルコンテンツの知的所有権の確保や著作権侵害（不正コピーや再配布など）の防止は重要な課題である．著作活動は古くから人間が営んできた文化的活動であり，デジタルコンテンツの不正利用の問題を解決することは将来の知的基盤社会を支える鍵となると考えられる．

デジタルコンテンツの著作権保護の手法として，重要な情報（著作権情報や利用者の ID）を不正な人間やシステムに知覚できないよ

うにデジタルコンテンツに埋込む『電子透かし技術』が注目を集めている．

電子透かし技術の中でも，不正コピーや不正再配布を防止するために個々のコンテンツに利用者の ID 情報を電子透かし手法を用いて埋め込む技術は特に『デジタル指紋』と呼ばれる．この技術により，

（ｉ）不正行為を行った不正者を積極的に追跡出来る
（ii）不正行為への抑止力となる

などの，通常の電子透かし技術では対処できない多くの利点を持つ．

デジタル指紋の手法では，複数人の不正者が結託して自分の ID 情報を改ざんさせる『結託攻撃』が可能となり，この攻撃に対して耐性を持たせることが大きな課題となる．この目的のために誤り『訂正符号』などの通信路符号化技術を用いたデジタル指紋符号が 1998 年に初めて提案され，この研究が引き金となって様々な特性を持つ符号化法が提案されている．

２．研究の目的

従来のデジタル指紋に関する研究では，（ｉ）不正者のデジタル指紋系列（符号語）の各シンボルからひとつのシンボルが選ばれる結託攻撃モデル『シンボル選択攻撃』，（ii）不正者のシンボルが平均化される結託攻撃モデル『平均化攻撃』などの攻撃法が主に考えられている．シンボル選択攻撃に対し，ある閾値以下の不正者のうち少なくとも一人は検出できる符号として，Frame-Proof 符号や Traceability 符号等が挙げられ，様々な構成法が提案されている．また，平均化攻撃はマルチメディアコンテンツのデジタル指紋に対する有効な攻撃法として，盛んに研究されている．平均化攻撃に対して耐性を持つ符号の中では，W. Trappe らによる符号が先駆的な存在である．この符号は，不正者の数がある閾値以下のときに全ての不正者の検出を保障できる点に最大の特徴がある．しかし，これらの符号の符号長に対する符号語数の割合（デジタル指紋システムの『効率性』をはかる指標となる）はまだまだ低く，実用化に向けてはこの点を解決することが必要である．そこで特にマルチメディアの保護のためのデジタル指紋符号システムの実用化を目指し，本研究では以下の点を目的とする．

(1) デジタル指紋符号の効率化と低計算量で実行可能な復号アルゴリズムの開発
(2) マルチユーザ通信路における符号との関連性の解明

従来の研究では特定の攻撃法を仮定して，その攻撃法に有効なデジタル指紋符号を設計することが多い．一方，実際には不正者は様々な攻撃法を検討できるため，実用化の際には様々な攻撃モデルに対して耐性を持つ符号をそれぞれ用意して，保護対象のコンテンツに埋め込む必要がある．したがって，実用化を目指す際には，ひとつの符号化法で多くの攻撃法に耐性を持つことが求められる．本研究では，従来考えられている複数の結託攻撃に耐性を持つ統一的な符号化法を開発することを最終的な目標とする．

３．研究の方法

(1) デジタル指紋符号の効率化と低計算量で実行可能な復号アルゴリズムの開発

従来の攻撃モデルに対して耐性を持つ符号の効率よい『復号アルゴリズム』（不正者の検出アルゴリズム）を開発する．例えば W. Trappe らが提案した符号の復号には，基本的に全ての符号語の組み合わせを探索することが必要となるが，この方法では符号語数が大きくなるにつれて，指数的に計算量が増大する．したがって，システムの効率化を図るほど（符号語数を増やすほど）逆に復号アルゴリズムの計算量が増大する問題が起こる．そこで，誤り訂正符号の復号アルゴリズムのように符号長の多項式オーダの計算量で実行できるアルゴリズムの開発を目指す．なお，誤り訂正符号を用いた通信システムでは，符号長の多項式オーダの計算量で実行できる復号アルゴリズムを持つ符号のみが，実際の通信システムに用いられている．このため，上記の視点は実用化にむけて非常に重要となると言えよう．

さらに，実際のシステムを考えたときには，システム雑音など保護対象のコンテンツにランダムに起こる誤りに対する耐性も重要である．そこで，コンテンツに誤りが起こったときにも，不正者の検出誤り率を出来るだけ小さく抑えられる符号化法も併せて検討する．

(2) マルチユーザ通信路における符号との関連性の解明

不正者に攻撃されたコンテンツから不正者を推定する過程は『マルチユーザ通信』における符号化システムと類推することができる．マルチユーザ通信とは，情報の送信機・受信機が複数あるネットワーク型の通信路で，情報を誤りなく送信するための通信システムである．特に，複数の送信機から情報が送信される『多重アクセス通信』のモデルとの関係性は深いと考えられている．そこで，本研究で提案した符号化とマルチユーザ通信路における符号化の関連性を解明する．また，多重アクセス通信路やその他の関連するマルチユーザ通信路における符号化法を開発する．

本ステップにより，従来のマルチユーザ通信で用いられている符号化の考えがデジタル指紋符号に用いることが出来る可能性がある．その場合には，ステップ(1)に戻り，さらに良い符号化を検討する．

４．研究成果

(1) デジタル指紋符号の効率化と低計算量で実行可能な復号アルゴリズムの開発

マルチメディアのデジタル指紋に有用とされる『平均化攻撃』に対して耐性を持つ符号の効率性（符号長に対する符号語数の割合）を向上させる手法を提案した．特に，本研究分野で先駆的な存在である Trappe らの符号のクラスをより広いクラスに拡張し，従来の符号クラスでは構成できない優れた符号が存在することを示した(論文[2])．提案手法によって構成される符号は不正者の数がある閾値以下のときに全ての不正者の検出を保障できる．この点は Trappe らの符号の最大の特徴であり，提案した符号もこの特性を保ったまま，システムの効率性を向上させることができる．

また，同様に『平均化攻撃』を仮定したもとで，符号長に対して多項式時間で不正者の検出が可能な符号構成法を開発した．論文[2]の符号を強力な誤り訂正符号として知られる Reed-Solomon 符号と組み合わせることにより，符号の効率性は符号長に対して大幅に改善できる．一方，復号アルゴリズムの計算量も符号語数の増加に従って（符号長に対して準指数関数のオーダで）増大する．そこで，先に提案した符号化法に修正を施し，復号アルゴリズムを併せて統一的に開発することにより，符号長に対して多項式時間の計算量で実行できるデジタル指紋の符号化システムを実現した(学会発表[1])．構成される符号は論文[2]の符号と同様に，不正者の数がある閾値以下のときに全ての不正者の検出を保障できる．また，不正に作成されたコンテンツに雑音等の影響で誤りが起こった場合にも，誤り訂正の機能を持たせることが可能であることを示した．構成したデジタル指紋符号は組み合わせる Reed-Solomon 符号のパラメータを適切に設定すれば，誤り訂正能力を大きくすることができることを示した．この点は，システムの実用化の際には有用となると考えている．

論文[2]における符号の構成法では，強力な誤り訂正符号として近年注目されている LDPC 符号を構成する際に用いられるテクニックをベースにしている．また，学会発表[1]における提案手法では，Reed-Solomon 符号のリスト復号法をベースに復号アルゴリズムを開発している．このように，本研究におけるデジタル指紋符号の開発には，符号理論の分野で開発された手法が重要な役割を果たすため，誤り訂正符号の効率化，及び高性能な復号アルゴリズムの開発も併せて行った(論文[1],[3],[4])．

(2) マルチユーザ通信路における符号との関連性

デジタル指紋符号への応用を見据え，マルチユーザ通信における符号化に関する研究を行った．特に，相関のある並列通信路における符号化レートの限界（通信路量領域）の導出および符号の構成法を提案し，デジタル指紋符号との関連性を考察した(学会発表[3,4])．また，多重アクセス通信路における符号化システムに関する研究も行った．特に，送信機間の協調を許容する多重アクセス通信路における高性能な符号構成法を提案し，デジタル指紋符号との関連性を考察した(学会発表[2])．

本研究により，マルチユーザ通信（特に多重アクセス通信）とデジタル指紋符号の関係が多少明らかになった．この結果から，本研究で提案したデジタル指紋の符号化法が，逆にマルチユーザ通信における符号化法に用いることができる可能性が示唆される．例えば，符号長に対して多項式時間の計算量で復号が可能で，符号化レートの限界（通信路容量域）を達成できる符号のクラスは未だに見出されていない．一方，本研究で解明した両システムの関連性を利用すると，発表文献[1]における符号化法を多重アクセス通信路に応用することが可能となり，その際には本研究で示した計算量が実現できると期待している．

(3) 複数の結託攻撃に耐性を持つ符号化法の開発

従来の結託攻撃モデルの拡張とその攻撃に耐性を持つ符号の構成を検討した．特に，マルチメディアのデジタル指紋システムに対して有用な攻撃である『平均化攻撃』と汎用的データに対する研究で主に仮定される『シンボル置換攻撃』を統一的に表現する方法を検討した．さらに様々な攻撃方法を含む攻撃モデルを検討しているが，現時点では有効な解決手段が見いだせていない．この点はデジタル指紋符号の実現に向け，今後の大きな研究課題としたい．

５．主な発表論文等

〔雑誌論文〕（計４件）

[1] G. Hosoya, H. Yagi, M. Kobayashi, S. Hirasawa, ”Adaptive decoding algorithms for low-density parity-check codes over the binary erasure channel,”

(査読あり) IEICE Trans. on Fundamentals, vol.E92-A, no.10, pp.2418-2430, 2009年10月.

[2] H.Yagi, T. Matsushima, S.Hirasawa, “Fingerprinting codes for multimedia data against averaging attack,” (査読あり) IEICE Transaction on Fundamentals, vol.E92-A, no.1, pp.207-216, 2009 年 1 月.

[3] M.Kobayashi, H.Yagi, T. Matsushima, S. Hirasawa, “Density evolution analysis of robustness for LDPC codes over the Gilbert-Elliott channel,” (査読あり) IEICE Transaction on Fundamentals, vol.E91-A, no.10, pp.2754-2764, 2008年10月.

[4] Y. Sato, G. Hosoya, H. Yagi, S. Hirasawa, ”A method of grouping symbol nodes for shuffled BP decoding algorithm,” (査読あり) IEICE Transaction on Fundamentals, vol.E91-A, no.10, pp.2745-2753, 2008年10月.

〔学会発表〕(計4件)

[1] H.Yagi, ″Polynomial-time decodable fingerprinting codes for multimedia,” (査読あり) Proc. 2009 Mosharaka Intl. Conf. on Communications, Networking and Information Technology, Amman, Jordan, 2009年12月23日.

[2] H. Yagi, H. V. Poor, ″Coset codes for compound multiple access channels with common information,″ (査読あり) Proc. 2009 IEEE Int. Symp. on Information Theory, Seoul, South Korea, 2009年6月29日.

[3] H. Yagi, M. Kobayashi, S. Hirasawa, ″Random coding bounds for correlated parallel channels with unidirectionally cooperating decoders,″ (査読あり) Proc. Int. Symp. on Information Theory and its Applications (ISITA2008), pp.122-127, Auckland, New Zealand, 2008年12月8日.

[4] H. Yagi, T. Matsushima, S. Hirasawa, ″Error control codes for parallel channel with correlated errors″, (査読あり) Proc. of 2008 IEEE Information Theory Workshop (ITW'08), pp.421-425, Porto, Portugal, 2008年5月5日.

６．研究組織

(1)研究代表者

八木 秀樹 (Hideki Yagi)

電気通信大学・先端領域研究センター・特任助教

研究者番号： 60409737

(2)研究分担者　なし

(3)連携研究者　なし