様式 C-19

科学研究費補助金研究成果報告書

平成 23 年　4 月 27 日現在

機関番号：14501
研究種目：若手研究（B）
研究期間：2009～2010
課題番号：21760291
研究課題名（和文）　電子指紋によるトレーサビリティに関する研究

研究課題名（英文）　A Study of Traceability based on Digital Fingerprint

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（和文）：本研究では，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が有する不正者検出能力を一定の誤検出率の下で理論的に解析し，計算機シミュレーションによってその妥当性を確認した．また，従来想定されていた攻撃環境の制約を緩めて，より実環境に近い攻撃モデルにおいて解析を行い，より高い検出性能が得られる検出器を提案した．更には，検出能力を低下や通信コストの増加を抑えた上でこれらの方式を暗号プロトコルに実装する方法を考案した．

研究成果の概要（英文）：In this research, the actual traceability of spread-spectrum based fingerprinting scheme and collusion secure code with a constant and tiny false-positive probability has been analyzed both from the theoretical and experimental points of view. In the analysis, some constraints in attack strategies are relaxed to consider more realistic attack environment. Considering the effects caused by this attack, proper detectors that identify colluders involved in a pirated copy have been proposed to maximize the traceability. Furthermore, the procedure implementing the fingerprinting scheme in a cryptographic protocol has been proposed without seriously degrading the traceability and increasing the communication costs.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,900,000	570,000	2,470,000
2010 年度	1,500,000	450,000	1,950,000
年度			
年度			
年度			
総　計	3,400,000	1,020,000	4,420,000

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：電子指紋技術，CDMA 通信，結託攻撃，量子化誤差，結託耐性符号，AWGN 通信路

１．研究開始当初の背景

電子著作物の権利侵害は，YouTube に代表される動画配信サイトの急激な発展に伴って深刻な状況となっている．現在のところ対応策は，権利者による削除申請に依るところが大きい．それに対して技術的な解決策は従来より電子透かし技術を用いる方法が研究されている．その中でも利用者情報を電子的な指紋として埋め込む電子指紋技術は，大きな可能性を秘めた技術として注目を浴びている．しかし，利用者ごとに異なる情報を埋め込むために，同じコンテンツでも僅かに違

うものが存在する．複数人が結託してその違いを解析すれば，電子指紋が削除もしくは改変される恐れがある．このような攻撃を結託攻撃と呼ぶ．従来，結託攻撃への耐性を考慮する研究は，スペクトル拡散技術に基づく方式と結託耐性符号を用いる方式が考案されている．

申請者はこれまでに CDMA 技術を用いてスペクトル拡散技術に基づく方式を提案してきた．また，符号間干渉成分を逐次的に除去する手法を提案してきた．ただし，その結託耐性の評価は特定の環境のみであったため，あらゆる観点からの評価が不可欠である．結託耐性符号の研究においても攻撃環境の制約が厳しいものであった．

２．研究の目的

スペクトル拡散技術に基づく方式において，想定する環境の制限を緩めてより実環境に近い条件下において性能の評価を行う．また，それに伴って発見される従来手法の問題点の修正と理論的な解析を同時に行う．更には雑音の少ない環境において，どの程度の結託者数にまで耐性を有するのであるかを評価すると共に，効果的な検出器の考案を目的とする．

電子指紋技術には，実際に電子指紋情報をコンテンツに埋め込む分野と暗号プロトコルを用いた運用の分野がある．コンテンツの権利者がコンテンツに直接利用者の指紋情報を埋め込んで配布する場合，悪意のある権利者が自らコピーを流出させて，ある利用者の仕業に見立てる恐れがある．つまり，この場合，たとえ不正コピーを発見できて不正者を特定できたとしても，その事実を第三者に証明することはできない．この問題を解決するために暗号プロトコルを構築する必要がある．本研究では，スペクトル拡散技術に基づく埋め込み方式を暗号プロトコルに実装させるために必要な条件を調べ，その追跡能力を損なうことなく実装できる方式を考案する．

結託耐性符号においても同様に，従来から想定されていた攻撃環境の制約を緩めて，より実環境に近い条件を考慮して評価を行う．符号の各シンボルを電子透かし技術を用いてコンテンツに埋め込む場合に想定される影響を，通信路モデルに基づいて解析し，符号の結託耐性能力を評価する．

３．研究の方法

本研究では，スペクトル拡散技術に基づく電子透かし方式において，符号間干渉を逐次的に除去することにより生じる影響を解析的に調べ，その処理の最適化及び，効果的な検出器の設計を行う．スペクトル拡散技術に基づく方式では，最悪の攻撃は平均化攻撃であるとの報告がなされており，更に二次攻撃として雑音付加される場合が考えられている．そのため，平均化攻撃において埋め込まれている電子指紋信号がどのように減衰するのかを統計的に解析し，その理論値を求める．その減衰量に基づいて，検出可能な信号成分は結託者数の増加に伴ってどのように変化するかを理論的に解析する．

検出能力を評価する上で最も重要な要素は，誤って無実の利用者を検挙してしまう誤検出率である．本研究では誤検出率を一定とした条件の下で検出可能な不正者の数を評価する．この誤検出率は非常に低く設定する必要があるため，モンテカルロシミュレーションによって実験的に評価する場合には，その試行回数を非常に大きくする必要がある．そのため，複数の計算機サーバを並列で演算させてそのデータ収集を行う．

結託耐性符号の評価では，結託攻撃により生成した符号語にガウス雑音が付加された場合において提案する検出器がどの程度の性能を有するのかをモンテカルロシミュレーションによって調べる．

４．研究成果

スペクトル拡散技術に基づく電子指紋方式において，まずは雑音がない状況下で平均化攻撃のみを受けたコンテンツから不正者をどの程度検出できるかを調べたところ，100 人以上の結託攻撃においても，極めて高い精度で全員を一意に特定することが可能であった．通常電子指紋の信号成分は結託者数が c 人であれば，1/c に減衰するはずであり，ある程度の人数を超えると信号間の干渉成分の影響のため，検出が困難になると予測されるため，理論的だけでなく解析的に減衰量を調べた．

その結果，電子指紋情報を埋め込む際と結託攻撃の際に生じる量子化誤差の扱いによって，埋め込んだ信号の減衰量が劇的に変化することを発見した．指紋情報をコンテンツの周波数成分に埋め込む場合，空間領域に逆変換すると実数値となるため，量子化が必要となる．また，結託攻撃によって複数のコンテンツを用いて線形結託攻撃を行う場合にも同様に最終的には量子化処理が必要である．この前者と後者で行う量子化の処理方法の違いにより埋め込まれている指紋情報のエネルギー減衰量が劇的に異なる結果を得た(図 1 参照)．

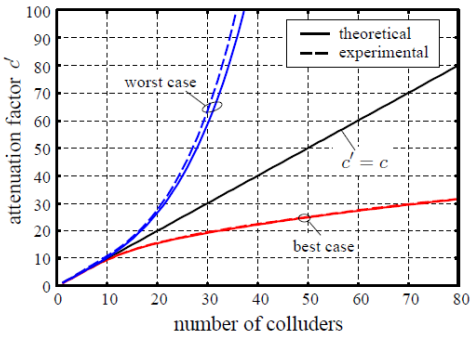

図 1. 電子指紋エネルギーの減衰量

この減衰が生じるメカニズムの理論的な解析を行い，その減衰量を制御する量子化法を考案した．計算機シミュレーションにより，量子化法による減衰量の違いを数値化し，提案量子化法により目標とした減衰量を満足する値が得られることを確認した．これらの成果により，スペクトル拡散技術を用いた電子指紋方式では，量子化法に気をつけなければ，設計した結託耐性能力が実際には低下する可能性があることを示すことができた．

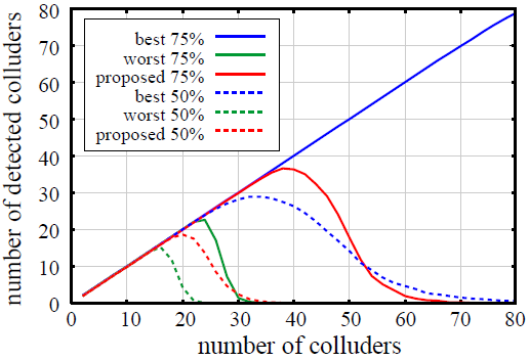

図 2. 提案量子化法による性能評価

この提案した量子化法を CDMA 技術に基づく電子指紋方式に適用させ，さらに暗号プロトコルに適用するための手法を考案した．この暗号プロトコルは，不正コピーの流出に関わった不正者を特定するだけでなく，その不正の事実を第三者に証明するために不可欠なプロトコルである．従来は，この暗号プロトコルの性質上，電子指紋情報をコンテンツに埋め込むために用いることが可能な電子透かし方式には特定のタイプに限られていた．本研究では，従来は難しいと考えられていたスペクトル拡散技術に基づく方式においても適用できるように，その手法に工夫を与えた．その結果，不正者追跡能力をほとんど損なうことなく暗号プロトコル上で実現することが可能となった．

一方，結託耐性符号として最近注目を浴びているTardos符号の構成法を解析し，カオス写像として有名なロジステック写像を用いれば簡単に実装できることを示した．また，検出能力を統計的な手法で解析し，検出できる不正者の人数の理論値を導出した．検出の際に計算する相関スコアは，統計的にガウス分布することが従来研究より発見されており，申請者はその分布を用いて無実のユーザを誤って検出する確率(誤検出率)を一定とする条件の下で，理論的に目標とするしきい値を計算する手法を提案した．設定した誤検出率に対して，検出できる不正者数の理論値の正当性を確認するため計算機シミュレーションを行い，実験値が理論値に極めて近い値を示すことを確認した．提案手法において作成した符号とオリジナルの符号との検出性能を比較するためにシミュレーションを行い，その妥当性を確認した．図3に符号長10000で結託者数が10人の場合における検出結果を示す．

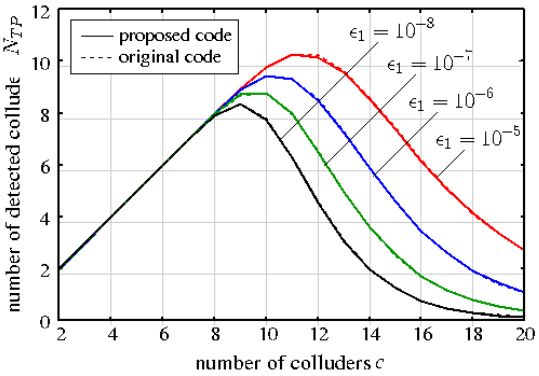

図 3. 検出された不正者数，符号長 10000，結託者数 10 人

従来は結託者間の符号の異なる位置のビットのみ自由に変更できるマーキング仮定に基づいた結託攻撃に対する耐性が議論されていた．しかし，実環境を考えると結託攻撃だけでなく信号処理などにより付加される雑音まで考慮する必要がある．そこで，本研究では白色ガウス雑音が付加されるモデルにおいて，結託耐性符号の追跡能力の変化を SNR に応じて求めた．その際に，不正コピーから抽出した符号語は雑音の影響のためアナログ信号となっている．そこで，誤り訂正符号の復号器で使われる硬判定と軟判定の手法を用いて新しい結託耐性符号の検出器を考案した．シミュレーションによりその性能を調べた結果，誤って無実のユーザを追跡してしまう冤罪確率が雑音の量に応じて増加することが確認された．そこで，雑音下においても一定となるように新しい検出器を設計し，その性能を調べた．雑音の影響を考慮していない検出器と考慮した検出器の性能を比較し，検出能力の結果を図 4 に，誤

検出率を図 5 に示す

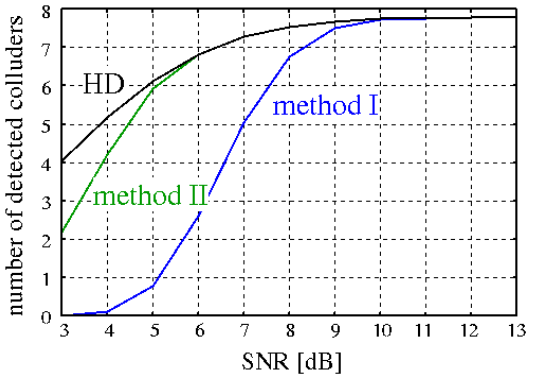

図 4. 雑音下における検出能力の比較，符号長 10000，結託者数 10 人

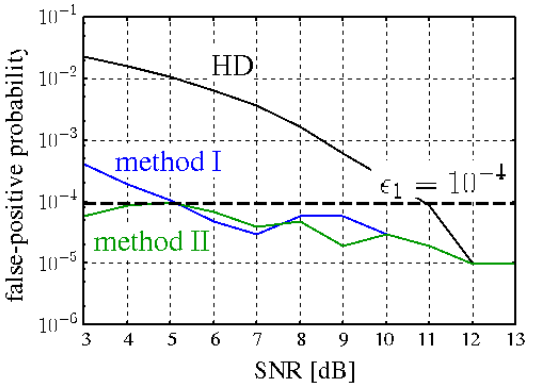

図 5. 雑音下における誤検出率の比較，符号長 10000，結託者数 10 人

これらの結果から，提案方式(method II)は検出能力をあまり損なうことなく一定の誤検出率で動作することが確認された．

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 6 件）

1. M. Kuribayashi, “Hierarchical spread spectrum fingerprinting scheme based on the CDMA technique,” EURASIP Journal on Information Security, vol.2011, Article ID 502782, 16 pages, 2011.

2. M. Kuribayashi and H. Kato, “Impact of rounding error on spread spectrum fingerprinting scheme,” IEEE Trans. Information Forensics and Security, vol.5, no.4, pp.670-680, 2010.

3. M. Kuribayashi, “Experimental assessment of probabilistic fingerprinting codes over AWGN channel,” 5th International Workshop on Security (IWSEC2010), LNCS 6434, Springer-Verlag, pp.117-132, 2010.

4. M. Kuribayashi, “Tardos’s fingerprinting code orver AWGN channel,” 12th Information Hiding Conference (IH2010), LNCS 6387, Springer-Verlag, pp.103-117, 2010.

5. M. Kuribayashi, “On the implementation of spread spectrum fingerprinting in asymmetric cryptographic protocol,” EURASIP Journal on Information Security, vol. 2010, Article ID 694797, 11 pages, 2010.

6. M. Kuribayashi and M. Morii, “Systematic generation of Tardos’s fingerprinting codes,” IEICE Trans. Fundamentals, vol.E93-A, no.2, pp.508-515, 2010.

〔学会発表〕（計 15 件）

1. M. Kuribayashi, “Hybrid Tracing Algorithm for Probabilistic Fingerprinting Code,” SCIS2011, 2011.

2. M. Kuribayashi, “Effect of Gaussian noise on the performance of binary fingerprinting code,” The 33th Symp. on Information Theory and its Applications (SITA2010), Dec. 2010.

3. M. Kuribayashi, “Experimental assessment of probabilistic fingerprinting codes over AWGN channel,” 5th International Workshop on Security (IWSEC2010), LNCS 6434, Springer-Verlag, pp.117-132, 2010.

4. M. Kuribayashi, “Reduction of interference for CDMA-based fingerprinting scheme based on random permutation,” The sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing

(IIHMSP2010), pp.494-497, 2010.

5. M. Kuribayashi,
"On the evaluation of spread spectrum fingerprinting," Computer Security Symposium 2010 (CSS2010), Oct. 2010.

6. M. Kuribayashi,
"Tardos's fingerprinting code orver AWGN channel," 12th Information Hiding Conference (IH2010), LNCS 6387, Springer-Verlag, pp.103-117, 2010.

7. 加藤寛史, 栗林稔, 森井昌克,
"電子指紋の結託耐性に有効な量子化方法の提案," 2010 年暗号と情報セキュリティシンポジウム (SCIS2010), 2010 年 1 月.

8. 門田宜也, 栗林稔, 森井昌克,
"結託攻撃を受けた Tardos 符号からの攻撃法の判別," 2010 年暗号と情報セキュリティシンポジウム (SCIS2010), 2010 年 1 月.

9. M. Kuribayashi,
"Tardos's fingerprinting code over AWGN channel," The 2010 Symp. on Cryptography and Information Security (SCIS2010), Jan. 2010.

10. M. Kuribayashi and M. Morii,
"Utilization of interleaver for CDMA-based fingerprinting scheme," The 32th Symp. on Information Theory and its Applications (SITA2009), Dec. 2009.

11. M. Kuribayashi,
"A study of traceability of CDMA-based fingerprint scheme," International Conference on Interaction Sciences (ICIS2009), pp.900-905, 2009.

12. M. Kuribayashi and M. Morii,
"Implementation of CDMA-based fingerprinting scheme in asymmetric fingerprinting protocol," Computer Security Symposium 2009 (CSS2009), Oct. 2009.

13. 加藤寛史, 栗林稔, 森井昌克,
"電子指紋技術における量子化誤差が与える影響の解析," コンピュータセキュリティシンポジウム 2009 (CSS2009), 2009 年 10 月.

14. 門田宜也, 栗林稔, 森井昌克,
"結託耐性符号の雑音による影響解析," コンピュータセキュリティシンポジウム 2009 (CSS2009), 2009 年 10 月.

15. M. Kuribayashi, H. Kato, and M. Morii,
"A study of rounding error on CDMA-based fingerprinting scheme," The Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2009), pp.1286-1289, 2009.

〔図書〕(計 1 件)
①. Kuribayashi,
"Recent fingerprinting techniques with cryptographic protocol," one chapter of "Signal Processing," Edited by Sebastian Miron," In-Tech Publisher, ISBN: 978-953-7619-91-6, Feb. 2010.

〔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
究者番号：50346235

(2)研究分担者

(3)連携研究者