様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　６月２９日現在

機関番号：５２６０１
研究種目：基盤研究（C）
研究期間：2009～2011
課題番号：２１５６０４２３
研究課題名（和文）　相関特性の優れたスペクトル拡散系列に基づく安全性の高い情報ハイディング技術の開発
研究課題名（英文）　Secure Information Hiding Technologies Based on Spread Spectrum Sequences with Good Correlation Properties
研究代表者
吉本　定伸　　（YOSHIMOTO SADANOBU）
東京工業高等専門学校・情報工学科・准教授
研究者番号：００３２１４０６

研究成果の概要（和文）：
理想的な相関特性をもつ完全相補系列を用いた情報ハイディング方式，具体的には，画像データを用いた電子透かし，電子指紋，ステガノグラフィ方式を考案し，その特性について計算機実験をもとに検証した。その結果，他のスペクトル拡散系列を用いた場合よりも，埋め込んだ秘密情報が画像に与える影響，秘密情報の抽出精度，攻撃への耐性などの面で優れていることが実証された。

研究成果の概要（英文）：
We developed information hiding technologies using complete complementary codes, one of the spread spectrum sequences with ideal correlation properties. Specifically, a digital watermarking scheme, a digital fingerprinting scheme, and a steganography scheme using image data are proposed. The properties of these schemes are evaluated through numerical experiments on the transparency of the secret information, correctness of the extraction and the robustness against various attacks. As a result, it is shown that the proposed schemes have superior to the method based on other spread sequences.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００９年度	1,100,000	330,000	1,430,000
２０１０年度	1,000,000	300,000	1,300,000
２０１１年度	900,000	270,000	1,170,000
年度			
年度			
総　計	3,700,000	1,110,000	4,810,000

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：暗号・セキュリティ，スペクトル拡散，系列生成，完全相補系列，情報ハイディング，電子透かし，電子指紋，ステガノグラフィ

１．研究開始当初の背景

(1) 社会的必要性と関連研究

情報ハイディングとは，デジタルコンテンツの中に，第三者に知られないように意図的に情報を隠す技術の総称であり，近年，著作権保護や不正配布防止技術をはじめ，秘密通信や電子投票などを実現する技術として注目を集めている。情報ハイディング技術の特性としては，耐雑音性や耐攻撃性に優れていることが要求される。このような技術で秘密情報が埋め込まれたデジタルコンテンツを不正利用するための代表的な攻撃方法とし

ては，故意にノイズや歪みを加えることによる秘密情報の劣化や，秘密情報の上書きによる消去，さらには，異なる秘密情報が埋め込まれたデータを比較したり平均化したりすることにより埋め込み情報を消去する結託攻撃などが挙げられる。

一方，無線通信に利用されるスペクトル拡散技術で用いられる拡散系列を，電子透かしなどに応用する研究例も報告されている。これらの研究では，スペクトル拡散技術の特性により，秘匿性や結託攻撃などに対する耐性をある程度高められることが示されている。スペクトル拡散技術においては，拡散系列の設計が非常に重要であり，相関特性の悪い系列を利用すると，マルチパスフェージングや局間干渉の影響を受けて，受信局における符号誤り率を著しく低下させることになりかねない。スペクトル拡散技術を電子透かしなどに応用した既存研究では，M 系列や Gold 系列といった系列が用いられることが多いが，これらの系列の相関特性は必ずしも理想的なものではなく，このことが耐雑音性や耐攻撃性をさらに向上させるための障害となっていることが考えられる。また，これらの系列の生成方式は非常に簡便であることから，埋め込みアルゴリズムを公開すると，秘匿性が著しく低下することも問題となる可能性がある。

(2) 既往研究の成果と着想に至った経緯

研究代表者らは，完全相補系列や ZCZ 系列と呼ばれる非常に相関特性の良い系列の設計方式や性能評価に関する研究に携わってきた。これらの系列の自己相関特性においては，0 シフト以外の特定区間における相関がゼロで，相互相関特性は同様の区間においてすべて 0 となる。研究代表者らのこれまでの研究では，このような特性を有する系列を近似同期 CDMA などの通信システムに応用することで，局間干渉やマルチパスフェージングが生じず，かつ周波数利用効率を飛躍的に向上できることが示されている。

このような研究成果を踏まえ，研究代表者らはこれらの系列を情報ハイディングに応用した場合，耐雑音性や耐攻撃性のさらなる向上を実現することができると考えた。一方，完全相補系列では，複数の系列を組み合わせることで初めて相関特性の直交性が保証される。この特性を利用し，秘密鍵をいくつかの要素に分割した後，完全相補系列で変調することで，すべての信号を決められた手続きで組み合わせないと鍵が復元できないという，安全な鍵配送方式を実現できると考えるに至った。

２．研究の目的

本研究の目的は，ZCZ 系列および相補系列など，相関特性の優れたスペクトル拡散系列を応用した情報ハイディング方式を開発し，その特性を評価することである。ZCZ 系列や完全相補系列を応用することで，耐雑音性や耐攻撃性を高めるだけではなく，秘密情報を多重化して埋め込むことができるものを目指す。また，送信者が透かしの埋め込まれたデータに故意に雑音を加えて送信し，受信側でこれらの系列を用いて雑音を除去できるような技術についても検討する。また，本方式で利用する秘密鍵情報を配送する方式についても検討する。

特性評価としては，開発した方式を画像や音声などのデータに導入し，埋め込みによるデータの劣化，耐雑音性に加え，結託攻撃を始めとする各種の攻撃に対する耐性を評価して，従来方式との性能比較を行う。さらに，これら技術面からの評価のみならず，利用者の視点に立った評価も行う。その方法として，提案技術を「技術者倫理」「工学倫理」「情報通信工学」などの講義における実践的な教材として利用し，学生が送信者，受信者，攻撃者などに分かれて実際に運用することで，安全性や実用性の評価を行う。

３．研究の方法

(1) ZCZ 系列および相補系列を用いた電子透かしアルゴリズムの開発および特性検証

従来のスペクトル拡散系列を利用した電子透かしアルゴリズムに対し，ZCZ 系列や完全相補系列などを導入する方法について検討する。本研究で使用する系列は，従来用いられてきた M 系列や Gold 系列とは系列の生成方法や特徴も大きく異なる。したがって，既存研究と同様の方法では容易に実装できないことが予想されるため，耐雑音性や耐攻撃性を高めるために効果的な導入方法について検討し，その効果を計算機シミュレーションなどで検証する。

また，必要に応じて，使用した系列を拡張したり，秘密情報の表現方法を変更したりすることで改良を加え，可視性や耐雑音性，耐攻撃性，および処理時間等に関する改善を試みる。特に，2 値系列のみならず，多相系列，すなわち多値複素系列を導入することを試みたり，完全相補系列の相関特性を計算するための高速手法などを導入することで計算負荷を軽減したりすることを検討する。

さらに，原画像参照型の電子透かし方式だけではなく，既存の原画像非参照型電子透かし方式に用いられている考え方を応用することにより，提案手法を原画像非参照型に拡張することも検討する。これら，改良方式についても，同様に数値実験を通した特性解析を行ない，埋め込み画像の可視性，耐雑音性，耐攻撃性，および秘密情報の埋め込みや抽出に要する時間などの観点から，既存方式や前

年度に開発した方式との比較検討を行う。
加えて，多数の秘密情報を同時に画像に埋め込む方式や，これを拡張したステガノグラフィ方式の特性検証や，電子指紋技術において多数の攻撃者により行なわれる結託攻撃への耐性に関する検証などについて，理論的考察および計算機実験の両面から実施し，必要に応じて，アルゴリズム等の改良を行なう。さらに，本方式に類似した情報ハイディング方式について提案されている改良法である QIM 法を提案方式にも適用し，その性能を評価し，情報理論的な考察を加えた上で，従来法との比較を行なう。

(2) 教育の現場で開発技術の評価を行なうためのシラバスの検討

本研究で開発した技術を実際の授業等で使用することで，利用者の視点で運用面での評価を行うことに備えて，「技術者倫理」「情報通信工学」などの講義や演習の中で，どのような方法で評価を行うのか，その内容や方式について検討する。その際，本方式の評価を適正に行うことができることに加え，学生への教育的効果についても十分に配慮する。必要に応じて，他高専や他大学における技術者倫理教育の実態調査なども行う。

これらの計画に基づき，高専本科および専攻科における「技術者倫理」「情報通信工学」の講義や演習などにおいて実際に使用する。講義や実習では，学生がそれぞれ送信者，受信者，攻撃者の役割に分かれて，秘密情報の送受信や攻撃を体験しながら，本方式の安全性や実用性について検証する。教材として使用するため，秘密情報の送信者と受信者，および攻撃者を想定して，それぞれ別々の PC を用いて既存のネットワーク設備とは独立した有線ネットワーク経由で通信を行なえる環境を整備する。

授業や演習の成果や学生へのアンケート調査の結果などをもとに，開発した技術の技術的および倫理的視点の双方から見た運用上の評価を行う。また，このような技術評価を教材として導入したことによる教育的効果についてもアンケートなどにより調査し，結果をまとめる。(3) 研究成果のまとめ

相関特性の優れた系列を応用した情報ハイディング方式の提案および特性検証に関する研究成果について，国内外の学会などで発表を行ない，論文の投稿も行う。また，研究成果をまとめ，関連する研究者らと将来的な研究の発展やさらなる問題提起を行なうことを目的としたワークショップを開催する。

４．研究成果

(1) 研究の主な成果

相関の良いスペクトル拡散系列として知られる完全相補系列を用いた電子透かし方式を考案し，その性能を計算機シミュレーションにより検証した。具体的には，ユーザ ID，グループ ID という二つの秘密情報を考え，これらを完全相補系列で表現し，画像データの周波数領域に埋め込むアルゴリズムと抽出するアルゴリズムを考案した。計算機シミュレーションにおいては，安全性として，画像への視覚的影響の有無や程度について検証した。また耐雑音性，耐攻撃性としては，秘密情報を埋め込んだ後の画像に雑音を付加したり，結託攻撃と呼ばれる秘密情報を消去する類の攻撃を加えたりした場合に，正しく秘密情報が抽出できるかどうかを検証した。これらの検証の結果，提案した方式は，M 系列や Gold 系列など，既存のスペクトル拡散系列を用いた電子透かし方式に比べて優れていることがわかった。

また，秘密情報の抽出時に原画像を参照しない，いわゆる「ブラインド方式」と呼ばれる電子透かしアルゴリズムを提案し，その特性評価を行なった。結果として，原画像の参照を行なう「プライベート方式」と比較すると，画像抽出時の相関関数における S/N 比がブラインド方式において 30dB 程度劣化するものの，ID の抽出は十分に可能であり，M 系列や Gold 系列など，他のスペクトル拡散系列を用いた場合と比較しても優位性を有していることが確認できた。また，電子商取引などにおいて，購入者の ID をデジタルコンテンツに埋め込む「電子指紋方式」へのアプリケーションを考慮し，提案方式が結託攻撃への耐性があるかどうかを，検出時に原画像を参照するプライベート型と参照しないブラインド型の双方について検証した。結果として，適切なパラメータを選択することにより．従来法に比べ飛躍的に結託耐性を向上できることを示した。ブラインド型では，QIM と呼ばれる方式を導入し，結託耐性が向上できることを示した。

また，提案方式は，自己相関特性のみならず，相互相関特性にも優れた系列を用いていることから，多数の秘密情報を同時に 1 枚の画像に埋め込むことを想定し，この場合の特性評価を行なった。これは，著作権者のリストを埋め込んだり，大きな情報を多重化して埋め込んだりするために有用であると考えられる。計算機実験の結果，必要なパラメータを適切に選ぶことにより，非常に低い抽出誤り率を実現できることが明らかとなった。このことを拡張して，一枚の画像に大量の情報を埋め込んで秘密通信を行なうステガノグラフィ方式を提案し，原画像を参照しないブラインド型のアルゴリズムを開発した。さらに，与えられたパラメータ設定の下で，1 枚の画像に埋め込むことができる最大の情報量を理論的に示し，計算機実験により，最大情報量に近いメッセージを埋め込んだ場

合，検出時にビット誤りが生じることを示した。これに対し，誤り訂正符号の一つであるLDPC符号を導入し，ビット誤りを0にできることを示した。

提案した情報ハイディング技術を教育現場で利用しながら評価するための方式について検討した。その結果として，利用者として高校生，高専生以下の学生を想定し，ゲーム感覚で情報ハイディングや提案技術について学ぶことができる教材を開発した。具体的には，画像に任意のメッセージを埋め込み，抽出を行なうアプリケーションや，透かし画像を劣化させることなく埋め込まれた秘密情報を取り除く攻撃ゲームアプリケーションを開発した。開発したアプリケーションは本校内でオープンキャンパスやセミナーの中で利用し，体験者に対してアンケート調査を行なうことでその効果を評価した。

研究の成果は，国際会議等で発表し，関連する研究者らと議論を深めた。2009年度および2011年度末には，ワークショップを開催して，研究成果発表を行ない，関連分野の研究者らと議論を深めた。

(2) 成果の位置付けとインパクト
および今後の課題

本研究で得られた成果，特に電子指紋方式とステガノグラフィ方式については，従来に知られてきた成果に対し優位性を持つ点で重要であると考えられる。電子指紋方式については，従来知られている方式よりも，大幅に検出可能な結託ユーザ数を増加させることに成功した意味で大きなインパクトを持つと考えられる。また，パラメータを調整することで結託耐性を向上させることができる点も重要である。一方で，配布可能なID数に上限があることは，本方式の大きな欠点であり，使用する系列やその生成方法等を工夫することで，ID数を向上させることが今後の大きな課題と言える。

一方，ステガノグラフィ方式については，従来知られているスペクトル拡散型のステガノグラフィ方式と同等の埋め込み律を達成した上，誤り訂正符号を導入することで，ほぼ100%に近い抽出成功率を達成することに成功した。しかも原画像を参照しないブラインド型でこれを達成したことは非常に重要である。その反面，原理的に埋め込み率をこれ以上向上することは現状では不可能であり，効率的な埋め込み方式や他の系列の併用などを考慮することで埋め込み率向上を図ることが今後の課題と言える。

また，本研究では，画像電子透かしに特化して研究を進めたが，今後は音声信号など他のメディアへの埋め込みを行ない，その特性検証を行なうことが必要であると考えられる。

５．主な発表論文等

〔雑誌論文〕（計2件）

1. Takahiro Matsumoto, Shinya Matsufuji, Tetsuya Kojima and Udaya Parampalli: ″Orthogonal and ZCZ Sets of Real-Valued Periodic Orthogonal Sequences from Huffman Sequences,″ IEICE Trans. on Fundamentals, vol.E94-A, no.12, pp. 2728－2736, 査読有 (Dec. 2011).

〔学会発表〕（計21件）

(1) Naoki Ohtani and Tetsuya Kojima: ″A Digital Fingerprinting Scheme Based on Complete Complementary Codes,″ 1st International Symposium on Technology for Sustainability, 2012年1月28日, Bangkok, Thailand.
(2) Tetsuya Kojima, Ryusuke Mayuzumi and Naoki Ohtani: ″Some Progresses on Information Hiding Strategies Based on Complete Complementary Codes,″ 第34回情報理論とその応用シンポジウム, 2011年12月2日, 岩手県雫石町.
(3) Ryusuke Mayuzumi and Tetsuya Kojima: ″A Blind Digital Steganography Scheme Based on Complete Complementary Codes,″ 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2011年10月14日, Dalian, China.
(4) Tetsuya Kojima, Naoki Ohtani, Takahiro Matsumoto and Udaya Parampalli: ″On Multiple Information Embedding by Digital Watermarking Based on Complete Complementary Codes,″ The Fifth International Workshop on Signal Design and Its Applications on Communications, 2011年10月11日, Guilin, China.
(5) Takahiro Matsumoto, Shinya Matsufuji, Tetsuya Kojima and Udaya Parampalli: ″A Generation Method of a ZCZ Set of Real-Valued Periodic Orthogonal Sequences from Huffman Sequences,″ The 2011 2nd International Conference on Innovative Computing and Communication and 2011 Asia-Pacific Conference on Information Technology and Ocean Engineering (CICC-ITOE2011), 2011年3月5日, Macau, China.
(6) Tetsuya Kojima, Naoki Ohtani, Takahiro Matsumoto and Udaya Parampalli: ″A Blind Digital Fingerprinting Scheme Based on Complete Complementary Codes,″ 2011 Australian Communications Theory Workshop, 2011年2月1日, Melbourne, Australia.
(7) Takahiro Matsumoto, Shinya Matsufuji,

Tetsuya Kojima and Udaya Parampalli: ″A Generation Method of an Orthogonal Set of Real-Valued Periodic Orthogonal Sequences from Huffman Sequences,″ 2011 Australian Communications Theory Workshop, 2011年1月31日, Melbourne, Australia.
(8) Tetsuya Kojima, Yoshiya Horii, Naoki Ohtani and Thierno Sene: ″On Some Properties of a Digital Watermarking Based on Complete Complementary Codes,″ 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2010年10月17日, Darmstadt, Germany.
(9) Tetsuya Kojima, Yoshiya Horii, Naoki Ohtani and Thierno Sene: ″On Properties of a Digital Watermarking Based on Complete Complementary Codes,″ 2010 IEEE International Symposium on Information Theory, 2010年6月16日, Austin, USA.
(10) Tetsuya Kojima, Yoshiya Horii, Naoki Ohtani and Thierno Sene: ″On Properties of a Digital Watermarking Scheme Based on Complete Complementary Codes,″ 電子情報通信学会情報理論研究会, 2010年1月8日, Honolulu, USA.
(11) Tetsuya Kojima and Yoshiya Horii: ″On Periodic Binary Complementary Sequence Sets Constructed by Complete Complementary Codes,″ 第32回情報理論とその応用シンポジウム, 2009年12月3日, 山口市.
(12) Ryusuke Mayuzumi and Tetsuya Kojima: ″A New Demodulation Procedure for CDMA Systems Based on Complete Complementary Codes,″ The Fourth International Workshop on Signal Design and Its Applications in Communications,
2009年10月22日, 福岡市.
(13) Yoshiya Horii and Tetsuya Kojima : ″On Digital Watermarks Based on Complete Complementary Codes,″ The Fourth International Workshop on Signal Design and Its Applications in Communications, 2009年10月22日, 福岡市.

〔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：
取得年月日：
国内外の別：

６．研究組織
(1)研究代表者
吉本　定伸 (YOSHIMOTO SADANOBU)
東京工業高等専門学校・情報工学科・准教授
研究者番号：００３２１４０６

(2)研究分担者
小嶋　徹也 (KOJIMA TETSUYA)
東京工業高等専門学校・情報工学科・准教授
研究者番号：２０２９３１３６

(3)連携研究者
松藤　信哉 (MATSUFUJI SHINYA)
山口大学・理工学研究科・准教授
研究者番号：００１７３８７３

(4)連携研究者
河村　豊 (KAWAMURA YUTAKA)
東京工業高等専門学校・一般科目・教授
研究者番号：１０３６９９４４

(5)連携研究者
飯作　俊一 (IISAKU SHUNICHI)
東京工業高等専門学校・情報工学科・教授
研究者番号：５０５４７８３３

(6)連携研究者
土居　信数 (DOI NOBUKAZU)
東京工業高等専門学校・情報工学科・教授
研究者番号：８０５４７８３６

(7)連携研究者
田中　晶 (TANAKA AKIRA)
東京工業高等専門学校・情報工学科・教授
研究者番号：２０５７８１３２

(8)連携研究者
松元　隆博 (MATSUMOTO TAKAHIRO)
山口大学・理工学研究科・助教
研究者番号：１０３０４４９５