

科学研究費助成事業 研究成果報告書

平成 28 年 6 月 29 日現在

機関番号：82727

研究種目：基盤研究(C) (一般)

研究期間：2013～2015

課題番号：25420396

研究課題名(和文) 誤り訂正符号の符号語の情報系列と検査系列の相関を利用した同期方式に関する研究

研究課題名(英文) A study on synchronization scheme using codeword stream generated by systematic error correction coding

研究代表者

山崎 彰一郎 (YAMASAKI, Shoichiro)

独立行政法人高齢・障害・求職者雇用支援機構職業能力開発総合大学校(能力開発院、基・その他部局等・教授)

研究者番号：60648963

交付決定額(研究期間全体)：(直接経費) 2,400,000円

研究成果の概要(和文)：本研究は、デジタル情報伝送における情報再生性能を向上させることを目的としている。固定パターンのビット系列を検出する同期処理において、ビット系列を保護する組織誤り訂正符号化が生成するパリティ成分の検査ビット系列を同期処理に適用し情報再生品質を向上させる方式を提案し、計算機シミュレーションにより有効性を確認した。さらに、無線通信システムにおいて盗聴端末が存在する環境で情報再生性能を強化する方式に拡張し、パケット通信で分散処理と符号化の前処理をともなう複数アンテナ送受信を用い、目標端末の情報再生性能を向上し、盗聴端末の情報再生性能を劣化させる方式を提案し、シミュレーションにより有効性を確認した。

研究成果の概要(英文)：This study improves the data transmission quality using systematic error correction coding. The detection of the inserted synchronization words is required to be robust against the transmission errors in wireless environments. The data stream is protected by error correction encoding and the codeword stream is transmitted. Assuming systematic encoding, the codeword stream consists of the data stream and the parity check stream. The detection performance of these inserted words is improved by using both the received data stream and the received parity check stream. The security enhancement is also required in wireless environments, since wireless communications are vulnerable to eavesdropping from unauthorized terminals. The secrecy performance of the packet communication is improved by using the information sharing and the precoded multi-antenna transmission.

研究分野：通信・ネットワーク工学

キーワード：デジタル情報通信 誤り訂正符号 同期 秘密分散 マルチアンテナ伝送

1. 研究開始当初の背景

無線環境のデジタル情報通信の受信機では、伝搬路における反射により遅延して到来する信号、他のユーザから到来する信号などが干渉として作用する。また、通信帯域が制限されることが多く、伝送情報は情報源符号化により圧縮された符号化ビット系列の形をとる。干渉などにより系列のビットに誤りが発生すると、情報源復号により再生される情報の品質が著しく劣化する。従って、情報再生品質の劣化要因となる各種の干渉に対する耐性の強化が必須となっている。

2. 研究の目的

無線通信において、情報再生品質を劣化させる各種の要因に対する耐性を強化することを研究目的とする。

(1) 映像情報を送信する際、情報源符号化により圧縮された符号化ビット系列は、フレームなどと呼ばれる短いビット系列に分割された構造になっており、そのフレームの先頭には、固定パターンのビット系列の同期ワードが、フレームの開始位置を定めるために挿入されている。受信機における情報再生では、受信ビット系列から同期ワードを検出する同期処理が前提となり、情報再生品質を高めるためには、ビット誤りのある受信ビット系列からの同期ワードの検出確率を高めることが必要となる。このため、同期ワード検出のビット誤りに対する耐性の強化をひとつの研究目的とする。

(2) 研究対象とする無線通信系を盗聴端末が存在し得る系に拡張すると、目標端末の受信条件を向上し、盗聴端末の受信条件を劣化させることが目標端末における情報再生品質を高めることになるため、盗聴に対する耐性を強化することもひとつの研究目的とする。

3. 研究の方法

符号化方式の効果的な利用が目的達成のための重要な方法となる。

(1) 無線通信では誤り耐性を強化するために、情報源符号化出力のビット系列に誤り訂正符号化を実施し符号語ビット系列を生成する。誤り訂正符号化が組織符号形式である場合、符号語ビット系列は情報ビット系列と検査ビット系列から構成される。

情報を再生するための同期処理において同期ワードを検出する際、通常は誤り訂正復号出力の情報ビット系列から同期ワードを検出する。本研究では、それに加えて、誤り訂正復号出力の検査ビット系列からも同期ワードを検出することにより、同期ワードの検出確率を高め、同期処理の誤り耐性を強化する。フェージング対策などのために用いられる複数アンテナ送受信においても、誤り耐性強化にトレリス空間時間符号化を実施すると、前記と同様に符号語系列は情報系列と検査系列から構成することができ、前記と同様の同期処理の誤り耐性の強化を実現する。

(2) 基地局から目標端末へ無線環境で情報をパケット形式で配信する系で、盗聴端末が存在することを想定する。パケット通信において、ペイロード情報の再生にはパケットのヘッダ情報の再生が必須となる。

ヘッダ情報を複数のパケットのヘッダに分散配置し、符号化による前処理をとともう複数アンテナ送受信を実施することにより、目標端末の受信条件を向上させ、盗聴端末の受信条件を劣化させ、盗聴に対する耐性の強化を実現する。

4. 研究成果

(1) 評価映像ソースに対して、MPEG-4方式の映像符号化機が生成する符号化ビット系列に、組織畳み込み誤り訂正符号化を実施し、情報ビット系列と検査ビット系列から構成される符号語ビット系列を生成し、この系列を多値の送信シンボルに変換し、定常伝送系あるいは、時変伝送系の伝送路上で、単数送受信アンテナ、あるいは、複数送受信アンテナで伝送し、受信シンボルを受信符号語ビット系列に変換し、誤り訂正復号の後、MPEG-4映像復号機が映像を再生する計算機シミュレーション評価系を構築した。

(2) MPEG-4映像符号化ビット系列は、誤り伝搬を抑制するために、短い系列に区切ったフレーム構造になっており、フレームの先頭には同期ワードが挿入されている。誤り訂正復号出力のビット系列には残留誤りが存在することが多く、残留誤りを含むビット系列から、同期ワードを正しく検出することが映像情報再生品質の向上に必須となる。

誤り訂正復号出力の情報ビット系列から同期ワードを検出する従来方式と、誤り訂正復号出力の情報ビット系列と検査ビット系列の両方から同期ワードを検出する提案方式を前記計算機シミュレーション系の単数アンテナ送受信系で評価した結果、提案方式における同期ワードの検出確率の向上が確認された。また、図1に示す従来方式で再生した映像フレームと図2に示す提案方式で再生した映像フレームを比較すると、映像再生品質の視覚的な向上が確認される。複数アンテナ送受信系においては、時変伝送における特性の改善を図る目的で、トレリス状態制御を行う提案方式の効果を確認した。



図1: 従来方式



図2: 提案方式

(3) 無線通信システムにおいて、盗聴端末が存在し得ることを考慮し、目標端末における情報再生品質を向上し、かつ、盗聴端末における情報再生品質を劣化させる技術の開発

に研究を拡張し、前記の計算機シミュレーション評価系を、送信側である基地局と、受信側である目標端末と盗聴端末から構成される系に拡張した。

パケット通信では、パケットのヘッダ情報の完全な受信が必須である。目標端末ではヘッダ情報の受信特性を向上させ、盗聴端末ではヘッダ情報の受信特性を劣化させることにより、盗聴に対する耐性を強化する。このために、ヘッダ情報を (k, n) しきい値法の秘密分散方式により n 個の分散情報に分割し、 n 個のパケットのヘッダに分散配置する。この秘密分散方式において、ヘッダ情報の再生には、 k 個以上の分散情報が必要で、 k 個未満の分散情報ではヘッダ情報は全く再生されない。

符号化による前処理をともなう複数アンテナ送受信で、目標端末では受信条件を向上させパケットに収容された k 個以上のヘッダの分散情報の再生を容易にし、一方、盗聴端末では受信条件を劣化させパケットに収容された k 個以上のヘッダの分散情報の再生を不可能とする方式を提案した。ヘッダ情報の再生確率の評価により、盗聴に対する耐性の強化を確認した(引用文献)。

以上述べたように、本研究では、無線通信系の情報再生品質の向上の目的に対し、符号化方式を基礎とした技術により耐性を強化する研究を進めた。計算機シミュレーション評価系を開発し、提案方式の効果を確認した。
<引用文献>

Shoichiro Yamasaki, Tomoko K. Matsushima, A security enhancement technique for wireless communications using secret sharing and physical layer secrecy transmission, IEICE Transactions on Information and Systems, Vol.E99-D, No.4, 2016, pp.830-838.

5. 主な発表論文等

[雑誌論文](計1件)

Shoichiro Yamasaki, Tomoko K. Matsushima, A security enhancement technique for wireless communications using secret sharing and physical layer secrecy transmission, IEICE Transactions on Information and Systems, 査読有, Vol.E99-D, No.4, 2016, pp.830-838. DOI: 10.1587/transinf.2015ICP0010

[学会発表](計27件)

Shinichiro Miyazaki, Tomoko K. Matsushima, Shoichiro Yamasaki, Kotoku Omura, A visible-light communication system using optical CDMA with RGB multi-chip LEDs, 15th International Symposium on Communications and Information

Technologies (ISCIT), 査読有, 2015年10月7日~9日, 奈良春日野国際フォーラム (奈良県・奈良市).

山崎彰一郎, 松嶋智子, 宮崎真一郎, 物理層の情報保護と秘密分散を用いた通信方式の検討, 電子情報通信学会2015年ソサイエティ大会, B-20-7, 2015年9月8日~11日, 東北大学, (宮城県・仙台市).

宮崎真一郎, 松嶋智子, 山崎彰一郎, 拡張プライム系列を用いたCDMA無線通信のための多重ユーザ干渉除去方式, 電子情報通信学会 情報理論研究会, IT2015-19, 2015年7月13日~14日, 東京工業大学, (東京・目黒区).

Shoichiro Yamasaki, Tomoko K. Matsushima, Shinichiro Miyazaki, Secure wireless communications using secret sharing and vector coding, 2014 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 査読有, C2L-A-05, 2014年11月17日~20日, ANA インターコンチネンタル石垣リゾート (沖縄県・石垣市).

Shinichiro Miyazaki, Shoichiro Yamasaki, Ryuji Kohno, Performance evaluation of single carrier transmission using frequency domain equalization, 2014 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS), 査読有, A3P-D-09, 2014年11月17日~20日, ANA インターコンチネンタル石垣リゾート (沖縄県・石垣市).

Kotoku Omura, Shoichiro Yamasaki, Tomoko K. Matsushima, Hirokazu Tanaka, Miki Haseyama, Performance of error resilient method using invertible codes for 3D DWT video transmission, 29th International Technical Conference on Circuit/Systems Computers and Communications (ITC-CSCC), 査読有, PID 1122, 2014年7月1日~4日, Phuket(Thailand).

Hirokazu Tanaka, Shoichiro Yamasaki, Tomoko K Matsushima, Miki Haseyama, A study on simplified structure for multi-carrier DS-CDMA with bi-orthogonal keying, 29th International Technical Conference on Circuit/Systems Computers and Communications (ITC-CSCC), 査読有, PID 1063, 2014年7月1日~4日, Phuket (Thailand) .

山崎彰一郎, 松嶋智子, 大野成義, 組織 Reed-Solomon 符号を用いた秘密分散法とその応用について, 電子情報通信学会 IT/ISEC/WBS 合同研究会, IT2013-88, 2014年3月10日~11日, 名古屋大学 (愛知県・名古屋市).

宮崎真一郎, 山崎彰一郎, 河野隆二, 周波数領域等化を用いたシングルキャリア伝送の性能評価, 電子情報通信学会 IT/ISEC/WBS 合同研究会, IT2013-90, 2014年3月10日~11日, 名古屋大学 (愛知県・名古屋市).

山崎彰一郎, 松嶋智子, 大野成義, 秘密分散とプリコーディングを用いたパケット無線通信の情報保護方式, 電子情報通信学会 スマートインフォメディアシステム研究会, SIS2013-51, 2013年12月12日~13日, とりぎん文化会館 (鳥取県・鳥取市).

Shoichiro Yamasaki, Tomoko K. Matsushima, A compression scheme of secret sharing, 2013 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 査読有, WA2-D-3, 2013年11月12日~15日, 沖縄県市町村自治会館 (沖縄県・那覇市).

Kotoku Omura, Shoichiro Yamasaki, Tomoko K. Matsushima, Hirokazu Tanaka, Miki Haseyama, Error resilient 3D DWT video transmission using invertible codes, 2013 International Symposium on Intelligent Signal Processing and Communication Systems (ISPACS), 査読有, WA1-B-5, 2013年11月12日~15日, 沖縄県市町村自治会館 (沖縄県・那覇市).

Tomoko K. Matsushima, Shiho Sasaki, Masaki Kakuyama, Shoichiro Yamasaki, Yuya Murata, Yasuaki Teramachi, A visible-light communication system using optical CDMA with inverted MPSC, Sixth International Workshop on Signal Design and Its Applications in Communications (IWSDA), 査読有, 4-4, 2013年10月27日~11月1日, 機械振興会館 (東京都・港区).

Shoichiro Yamasaki, Tomoko K. Matsushima, Hirokazu Tanaka, A state transition control method of space-time trellis coded transmission, 2013 International Workshop on Smart Info-Media 2013

International Workshop on Smart Info-Media Systems in Asia (SISA), 査読有, RS1-5, 2013年9月30日~10月2日, 産業労働センターウインクあいち (愛知県・名古屋市).

山崎彰一郎, 松嶋智子, 秘密分散情報の符号化に関する研究, 電子情報通信学会 スマートインフォメディアシステム研究会, SIS2013-51, 2013年9月12日~13日, 早稲田大学(東京都・新宿区).

大村光徳, 山崎彰一郎, 松嶋智子, 田中宏和, 長谷山美紀, 3D DWT ビデオ伝送のビット誤り耐性の強化, 電子情報通信学会 スマートインフォメディアシステム研究会, SIS2013-14, 2013年9月12日~13日, 早稲田大学(東京都・新宿区).

大村光徳, 山崎彰一郎, 松嶋智子, 田中宏和, 長谷山美紀, インバーティブル誤り訂正符号を利用した 3D DWT ビデオ伝送の誤り耐性強化, 電子情報通信学会 情報理論研究会, IT2013-21, 2013年7月25日~26日, 早稲田大学(東京都・新宿区).

山崎彰一郎, 大村光徳, 松嶋智子, 田中宏和, 時空間符号化伝送の誤り制御方式の検討, 電子情報通信学会 スマートインフォメディアシステム研究会, SIS2013-2, 2013年6月13日~14日, 鹿児島県文化センター宝山ホール(鹿児島県・鹿児島市).

6. 研究組織

(1) 研究代表者

山崎 彰一郎 (YAMASAKI, Shoichiro)
独立行政法人高齢・障害・求職者雇用
支援機構職業能力開発総合大学校・能
力開発院・教授
研究者番号：6 0 6 4 8 9 6 3

(2) 研究分担者

松嶋 智子 (MATSUSHIMA, Tomoko)
独立行政法人高齢・障害・求職者雇用
支援機構職業能力開発総合大学校・能
力開発院・教授
研究者番号：3 0 6 4 8 9 0 2

宮崎 真一郎 (MIYAZAKI, Shinichiro)
独立行政法人高齢・障害・求職者雇用
支援機構職業能力開発総合大学校・能
力開発院・助教
研究者番号：4 0 6 4 8 9 3 7

(3) 研究協力者

田中 宏和 (TANAKA, Hirokazu)