様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　６ 年　 ６ 月 １６ 日現在

機関番号：３２５１５
研究種目：基盤研究(C)（一般）
研究期間：2018～2023
課題番号：１８Ｋ１１３０１

研究課題名（和文）音響データへの情報秘匿のブラインド検出

研究課題名（英文）Blind detection of audio data hiding

研究代表者
西村　明（Nishimura, Akira）

東京情報大学・総合情報学部・教授

研究者番号：３０２８６１８２

交付決定額（研究期間全体）：（直接経費）　　2,700,000円

研究成果の概要（和文）：音データへの情報秘匿の有無を、秘匿前の音データ無しでブラインド検出する手法を複数検討した。音波形データの最下位ビットに情報秘匿する手法に対しては、最高周波数近傍のエネルギー時間変化の統計量を用いて検出が可能であった。一方、2019年に公開された 10,000ファイルの音楽データである Audio Steganalysis Dataset に対しては、上記手法は無効であった。このため検査対象信号に対して情報秘匿を行い、その秘匿前後の差異から、秘匿の検出が可能な信号を選別する手法を開発した。AMR音声符号化データへの情報秘匿に対しては、符号化データの統計的性質を基に既存手法より高い検出率を得た。

研究成果の学術的意義や社会的意義
ディジタルコンテンツへ情報を秘匿する技術は、インターネット上の様々なコンテンツへ機密情報を秘匿できるため、テロリストや犯罪組織の秘匿通信に使われている、という疑いがある。これを検出するため、情報秘匿前のコンテンツ無しに、情報秘匿の有無を検出する手法である、ステガナリシスの必要性が高まっている。なかでも Steghide による情報秘匿に対しては、これまで多様な音データに対しての有効なステガナリシスが示されていなかった。本研究は Steghide に対してのステガナリシスの適用可能な音データの特徴を明示することで、適用不可能な音データに対する今後の課題も示した。

研究成果の概要（英文）：Several methods to blindly detect information hiding are investigating whether the information is hidden in audio data without the audio data before hiding. For a technique that hides information in the least significant bit of audio waveform data, the detection was possible using the statistics of temporal energy change near the highest frequency. However, the above methods were ineffective for the Audio Steganalysis Dataset, released in 2019, containing music data of 10,000 files. For this reason, we developed a technique to inspect the signals for testing and select signals in which hiding can be detected based on the difference before and after hiding. For information concealment in AMR speech coding data, a higher detection rate than existing methods based on the statistical properties of the coded data was proposed.

研究分野：音響情報処理

キーワード：情報ハイディング　ステガノグラフィ　ステガナリシス　音響信号データセット　機械学習　音声符号化　振幅変動統計量　最下位ビット

様　式　Ｃ－１９、Ｆ－１９－１（共通）

１．研究開始当初の背景

ディジタルコンテンツへ任意の情報を秘匿し検出して活用する情報秘匿（情報ハイディング、電子透かし）技術が悪用される危険性が指摘されている。例えば、一般的な画像や音のコンテンツに犯罪・テロ組織が秘密通信情報を秘匿するものである。既存の通信チャネルを用いた暗号通信では、通信の事実を隠ぺいすることは難しいが、任意のコンテンツを改ざんして情報を秘匿する場合、改ざんは見た目では分からず、誰がどこで発信して誰が受信しているかも不明で、高度化するサイバー犯罪の摘発を困難にしている。

このようなコンテンツファイルへの改ざんを検知するには、電子署名やハッシュを用いることができる。しかし、情報を秘匿していないオリジナルコンテンツが公に存在しない場合、例えば、一般ユーザが撮影・録音・制作し公開するコンテンツファイルに対しては無効である。

よって、コンテンツデータをスキャンして情報秘匿の有無を検出すべきであり、そのような分析をステガナリシスとよぶ。画像データに対しては情報秘匿の研究とステガナリシス研究が比較的多く行われているが、音響データに関しては、音響と画像のデータ特性の違いに起因するその技術達成の困難さもあり、ステガナリシス研究は相対的に少ない。

２．研究の目的

音響データへの様々な秘匿方法を用いた情報秘匿の有無を、秘匿前の信号なしで検知するブラインド検知は可能であるのか、音響情報秘匿技術の悪用を検知し防ぐための、情報秘匿の有無をブラインド検知する技術（ステガナリシス）の開発・評価を、本研究の目的とした。

３．研究の方法

(1) Steghide 情報秘匿手法に対するステガナリシス

音響波形信号の最下位ビットの一次統計量への影響を最小限にした情報秘匿手法 Steghide に対するステガナリシスを対象とする。従来ステガナリシス手法を概観し、それらの研究では対象とする音響信号が公開されていないため、どのような音響信号の特徴がステガナリシスの手掛かりになっているかが明示されていない問題点を指摘する。そのため、従来法を実装したシミュレーション実験を実施し、秘匿対象信号の高周波数成分の統計量を利用することで、高い検出性能が得られていることを示す。また、音声信号に対する、背景雑音の重畳強度とアンチエリアシングフィルタの特性の、検出性能への影響を明らかにする。さらに高周波数成分の統計量を効果的に利用するステガナリシスを提案し、従来法と検出性能を比較する。

(2) 下位ビット値予測手法の開発とそれを利用したステガナリシス

前述の Steghide による情報秘匿は、最下位ビット値が秘匿ビット値に等しくなるように、サンプル値の入れ替えが行われるため、最大で 25%程度の振幅値が本来の最下位ビット値とは異なる値に変更される。このため、線形量子化音響信号の振幅上位ビット値を用いて、下位ビット値の予測を行う手法を開発し、最下位ビット値を予測した際の予測正解率の変化により、Steghide による情報秘匿の有無を検出する。

(3) AMR 音声符号化データへの情報秘匿に対するステガナリシス

携帯電話で用いられている CELP(Code Excited Linear Prediction) 音声符号化は、5～10 ms のサブフレーム毎にピッチ周期を求め、量子化する。3G/4G 携帯電話音声およびヴォイスレコーダ等で主に用いられている、AMR 符号化は CELP の一種であり、1 フレームは 20ms、これを 4 つのサブフレームに分割する。ビットレートは, 4.75 kbps から 12.2 kbps までの 8 つのモードをもつ。12.2 kbps モードは、奇数サブフレームでピッチ周期を量子化し、偶数サブフレームは直前の奇数サブフレームのピッチ周期からの偏差 -5 3/6 から +4 3/6 1 サンプルの範囲を 1/6 サンプルの精度で直線量子化する。この偶数サブフレームのピッチディレイ値のヒストグラムを得ると、3 点周期のピークが見られる。情報秘匿を行うと、これらのピークが小さくなるため、これを機械学習により検出する新たなブラインド検出手法の効果を、情報秘匿に伴うピッチ揺らぎを学習する従来法との比較を含めて示す。

情報秘匿手法としては、ピッチディレイ探索範囲を、秘匿するデータビット値に応じて偶数範囲か奇数範囲かに限定し、10 サブフレームあたり秘密鍵に基づいてランダムに n フレームを選択して 200×n×0.1 bps の埋め込みを行う RPQ (Randomly selected Pitch Quantization) 法と、連続する奇数サブフレームのピッチ周期が大きく(±10% 以上)変化する部分について、これ

ら奇数サブフレームに挟まれる偶数サブフレームのピッチ周期の値について、同様にランダムな位置のビット値を秘匿情報と置き換える RPCP（Randomly selected Pitch Change Point）法の二つを対象とした。

(4) Audio Steganalysis Dataset への情報秘匿に対するステガナリシス

これまでの一連の研究では、情報秘匿対象となる音響信号の特性（ナイキスト周波数付近のパワー、信号の振幅、背景雑音の有無など）によって、ステガナリシスの精度が異なることが示されてきた。本研究課題開始後の 2019 年、音楽信号のステガナリシス向け研究用データベースとして、IEEE Dataport において、Audio Steganalysis Dataset が公開された。これには、44.1kHz サンプリング、16-bit 量子化された 10 秒間の WAV ファイルが 10,000 個含まれている（Medium Dataset）。これに対して、Steghide のステガナリシスが成功した、という報告は 2023 年時点で無かった。

本報告(1)節にて開発した手法および小振幅部分の強度変化に着目した手法も、このデータセットに対しては、F 値 0.6 程度の検出性能しか達成できず、困難を極めた。そこで、情報秘匿の有無の検査対象となる信号が、ステガナリシスに適する（成功する）信号がそうでないか、を事前に判別し、適する信号のみ小振幅部分の強度変化に着目した手法により、秘匿の有無を検出することとした。

４．研究成果

(1) Steghide 情報秘匿法に対するステガナリシス

従来ステガナリシス手法の概観とその特徴の分析、また一般的な秘匿対象信号である、音楽、音声、音声に重畳される背景雑音の周波数特性より、高周波数成分の統計量を利用することで、高い検出性能が得られることを示した。従来法を実装して、音声信号に対してシミュレーション実験を行うことで、重畳背景雑音の強度が強くなると検出性能が低下し、AD 変換時のアンチエリアシングフィルタが有効な場合、検出性能が向上することを示した。さらに高周波数成分の統計量を効果的に利用する新たなステガナリシスを提案し、従来法より検出性能がよいことも示した（図１）。また、情報秘匿量が未知である場合の検出性能を評価するため、検出モデルの学習時と検出時の情報秘匿量が異なる場合のシミュレーション実験も行い、秘匿量が少ない状態でモデルの学習を行うときに検出性能が高くなることも示した。

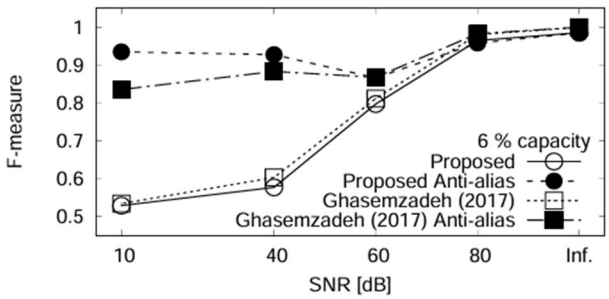

図１　音声への重畳雑音の SN 比に伴う、6% の情報秘匿量に対する、提案法と既存法との検出性能比較

(2) 下位ビット値予測手法の開発とそれを利用したステガナリシス

16 ビット信号の上位ビットを残し、下位ビットをゼロに置き換えた信号に予測下位ビット信号を加算し、その線形予測誤差信号を最小化するよう、予測下位ビット値の配置を疑似焼きなまし法により定めた。様々な音楽信号 100 種に対して、16 ビット振幅の上位 k ビット(8〜14)値を用いて次のビット値を予測した正答率を図２に示した。また、その客観音質劣化度合（ODG）を、従来のビット拡張法と比較し、提案法を用いることによる音質向上を確認した。この技術は、既存ディジタル音楽の小振幅部分で記録できなかった微小振幅を復元するハイレゾ化に有効であることが分かった。

当初の目的であった情報秘匿の有無の検出については、情報秘匿済み信号の下位ビット値の予測精度は、秘匿無し信号に対する予測精度と統計的に有意差が無かったため、不可能であることが分かった。その原因は、最下位ビット値の変更に伴いその上位ビット（第 3、および第 5 下位ビット）値も変更される場合があり、それが結果的に最下位ビット値の予測精度に変化を生じさせない要因となっているためであった。

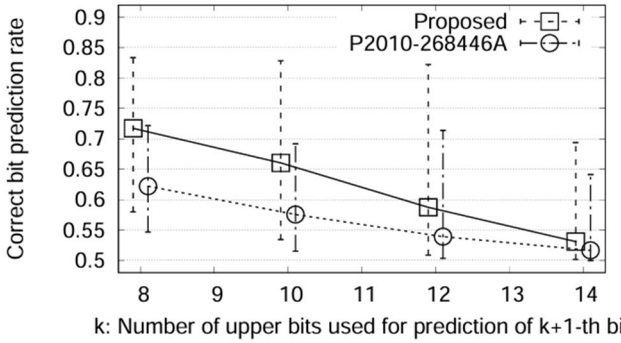

図２　従来法(特開 2010-268446A)と提案法の上位 k ビット値からの k+1 位ビット値の予測精度

(3) AMR 音声符号化データへの情報秘匿に対するステガナリシス

日本音響学会研究用連続音声データベース Vol.1 の全ての話者(男 30 名、女 34 名)の全ての発話を、30 秒づつ連結して 610 ファイル作成し、サンプリング周波数は 8kHz に変換した。音声信号には背景雑音(DEMAND Street Cafe 雑音) を重畳する条件を追加した。AMR 符号化には, 3GPPTS26.073 に付属している整数演算 ANSI-C コードと、これに情報秘匿用コードを付加したものを用いた。

表１は、従来法と提案手法の検出精度である F 値を、情報秘匿の割合と背景雑音との SN 比をパラメータとして示したものである。その結果、ほとんどの条件で提案手法が従来手法より検出性能が勝ることが分かった。従来法は背景雑音が重畳される場合や、偶数サブフレーム値のみが変更される場合に対して、性能が大きく低下することが分かった。

表１　実験条件ごとの 10 分割交差検証による平均 F 値

背景雑音	秘匿	識別手法	従来法		提案法	
SNR [dB]	割合 [%]	秘匿手法	RPQ	RPCP	RPQ	RPCP
∞	100		0.924	0.606	0.993	0.936
10	100		0.875	0.628	1.000	0.996
0	100		0.751	0.634	1.000	1.000
∞	20		0.714	0.593	0.703	0.816
0	20		0.662	0.581	0.770	0.968

(4) Audio Steganalysis Dataset への情報秘匿に対するステガナリシス

検査対象信号に新たに情報秘匿を行うと、それが既に情報秘匿されていた信号か否かに関わらず、秘匿前後のスペクトルに変化が生じ、検査対象信号への秘匿前後の振幅二乗コヒーレンスの最小値が変化することが分かった。こうして、Audio Steganalysis medium Dataset 10,000 ファイルのうち、27.3% が、情報秘匿の検出が可能なファイルと判定された。これらのファイルに対する、小振幅部分の秘匿に伴うパワー変化を特徴量としたステガナリシスによる検出精度は、秘匿有の正検出率が 93%、秘匿無しの正検出率が 97% であり、各段に検出精度を高めることができた。一方、情報秘匿の検出が不可能と判定された 72.7% のファイルに対しては、同じステガナリシス手法を適用しても 52.5%の正確性しか得られず、ほぼ検出不能であることが確認され、今後の課題となった。

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 西村明	４．巻 119
２．論文標題 音響波形への白色スペクトル加算的情報秘匿の有無識別	５．発行年 2020年
３．雑誌名 電子情報通信学会技術報告	６．最初と最後の頁 143-148
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Akira Nishimura	４．巻 11378
２．論文標題 A novel steganalysis of Steghide focused on high-frequency region of audio waveform	５．発行年 2019年
３．雑誌名 Lecture Notes in Computer Science : Digital Forensics and Watermarking	６．最初と最後の頁 69, 82
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-11389-6_6	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計7件（うち招待講演　1件／うち国際学会　2件）

１．発表者名 西村明
２．発表標題 ディジタル音響信号のサンプル置換による情報秘匿のブラインド検出
３．学会等名 日本音響学会春季研究発表会
４．発表年 2023年

１．発表者名 西村明
２．発表標題 音響法科学と録音属性推定
３．学会等名 電子情報通信学会EMM研究会（招待講演）
４．発表年 2022年

１．発表者名
西村明

２．発表標題
AMR音声符号化におけるピッチディレイへの情報秘匿のブラインド検出

３．学会等名
日本音響学会春季研究発表会

４．発表年
2022年

１．発表者名
Akira Nishimura

２．発表標題
Prediction of least significant bits from upper bits in linearly quantize d audio waveform

３．学会等名
AES 146th Convention（国際学会）

４．発表年
2019年

１．発表者名
Akira Nishimura

２．発表標題
A novel steganalysis of Steghide focused on high-frequency region of audio waveform

３．学会等名
Int. Workshop on Digital-forensics and Watermarking（国際学会）

４．発表年
2018年

１．発表者名
西村明

２．発表標題
音響波形の下位ビット置換による情報秘匿の有無識別における高周波数成分の効果

３．学会等名
電子情報通信学会EMM研究会

４．発表年
2018年

１．発表者名 西村明
２．発表標題 音響波形の下位ビット置換による情報秘匿の有無検出への背景雑音の影響
３．学会等名 平成30年秋季日本音響学会研究発表会
４．発表年 2018年

〔図書〕　計0件

〔出願〕　計1件

産業財産権の名称	発明者	権利者
音響信号処理方法及び音響信号処理装置	西村明	同左
産業財産権の種類、番号	出願年	国内・外国の別
特許、特願2019-026095	2019年	国内

〔取得〕　計0件

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関