マルティメディアデータを用いたステガノグラフィ

脇山正博，日高康展，河口英二*

A Prototype of Steganography System Using Multimedia Data

Masahiro WAKIYAMA, Yasunobu HITAKA and Eiji Kawaguchi*

Abstract

We are using Multimedia data such as Text data, Image data, Sound data and Video data through Internet. We explain Steganography system of information hiding by using the media data. We show the many algorithms of steganography system by basic approach of replacing the cover data in the least significant bits with secret data. This approach is that we express secret data in binary number, and replace them for the data on lower bit of dummy audio data. We used the audio part of wave file. The file format is a subset of Microsoft's RIFF specification for the storage of multimedia files. We implemented the steganography system and could embed the secret data using the method of low-bit coding. From now on, we will make the program. Our future assignment is to increase the capacity as well as improve the confidentiality of audio steganography.

Keywords : data hiding, low bits coding , Audio Steganography

1. はじめに

人間は有史以来，他人に気づかれること無く，自分の仲間とこっそりと意思の疎通を図る方法を捜し求めてきた．現代のステガノグラフィ[1]とは，秘密の情報が人目に触れないように，これを何か別の目立たないカバーデータと呼ばれる埋め込みデータの中に，こっそりと埋込む情報技術のことである．具体的には，画像データや音声データなどに秘密データを埋め込んで隠すことである．ステガノグラフィ技術自体は古くから利用されていたが，プログラムとしての歴史はまだまだ浅い．十数年前では一般ユーザが手軽に入手することのできるステガノグラフィ・プログラムは存在していなかった．しかし現在では研究も進み Web 上でプログラムを手に入れることは比較的容易になったといえる．しかしながら一般ユーザへのステガノグラフィの浸透度は低く，埋め込める秘密データの大容量化や秘匿性の向上などの課題も残されており，さらに研究を進める必要性がある．本論文では，第２章では，情報セキュリティシステムについて述べ，第３章では各メディアを用いたステガノグラフィについて述べ，第４章では実験について述べ，最後にまとめと今後の課題について述べる．

2. 情報セキュリティシステム

2.1 情報セキュリティ

情報セキュリティ技術とは，図１に示すように暗号化技術と情報ハインディングに分類される．情報ハインディングはさらに，ステガノグラフィと電子透かしに大別される．

１．暗号(Cryptgraphy)
２．情報ハインディング(Information Hinding)
ステガノグラフィ(Steganography)
電子透かし(Watermarking)

図1 情報セキュリティ技術

暗号とは，秘密通信のため当事者間の約束に基づいた平文に特定の変換処理を加えることである．情報の発信者が普通の平文に特定のアルゴリズムによる変換処理を加えることにより暗号化を行う．この暗号化された文を暗号文といい，アルゴリズムを暗号法といい，様々なアルゴリズムが存在する．暗号文は一見いかにも秘密情報が入っていると思われ，盗聴者には，その内容が理解できないようにしているが，この暗号文解読を解読して破ろうとする攻撃者の対象になりやすい．

情報ハインディングのステガノグラフィとは，ある秘密情報を別のものを使って隠す，あるいはある重要なことを別のものに忍ばせる，などと定義される．コンピュータ用語では，ある媒体となるデータを使って他のデータを隠す技術である．

電子透かしとは，主に著作権保護を目的とする技術である．「透かし」というと例えば紙幣に，それが本物であるかどうかの証拠として入れられている．このように価値のあるものの正真性や著作権を立証するための証拠を目立たない方法で付加しておく技術である．これは，写真データやグラフィックアート，音楽データなどのデジタル著作物を対象とするものである．表1にステガノグラフィと電子透かしとの違いを示す．

表1 ステガノグラフィと電子透かし

特徴	ステガノグラフィ	電子透かし
意味のある情報	外から見えない 埋め込まれた情報	外に現れた情報 (画像や音楽データ)
埋め込みデータの頑健さ	外から見えるデータを加工しようとすると容易に壊れて可	どのような処理がされても壊れないこと
埋め込みデータの復元条件	埋め込み前のデータを参照しない	埋め込み前のデータを参照して可
埋め込み容量	大容量	少量の目印程度

*九州工業大学名誉教授

電子透かし（Watermarking）は，画像や音楽等のデジタルコンテンツに情報を見た目にはわからないように埋め込む技術のことである．作者名，課金情報，コピー可能回数等を埋め込むことが多い．見た目にはわからないように情報を埋め込むという点では，ステガノグラフィと共通している．主にデジタルコンテンツの著作権保護を目的とする技術である．透かしという言葉の通り，お札に入っている透かしと同じで，コピーすることができず，著作権の保護に役立っている．コンピュータの世界では透かし自体をコピーされる可能性があるため，見た目にはわからないように，こっそりと透かしを埋め込む．これが電子透かしである．

一方ステガノグラフィは著作権の保護として使われることはない．ステガノグラフィでは埋め込む媒体となる情報には，何の価値も無いありふれた情報を使う．あくまでも重要なのは，埋め込む方の秘密情報である．また，電子透かしはごくわずかな量の情報を埋め込むが，ステガノグラフィは大量の秘密情報を埋め込むことが目的である．これらのことから，ステガノグラフィと電子透かしは本質的にまったく別のものであるということがいえる．

2.2　ステガノグラフィシステム

ステガノグラフィ(Steganography)とは，ある情報を別なものを使って隠したり，別なものに忍ばせたりするという意味を持つ．本論文ではコンピュータ上で取り扱われるデジタル情報を対象とし，秘密情報を別のダミー情報に隠蔽する．ステガノグラフィ自体はコンピュータの発明よりも遥か以前より使われているが，近年のコンピュータの急速な進歩により，大容量のデジタル情報に対しても容易に適用可能となった．

デジタル情報の伝送手段として今日最もよく利用されているインターネットは，その性質として第三者による盗聴を防ぐことが難しい．そのため，秘密情報を安全に伝達するには秘密情報の防衛技術が必須となる．ステガノグラフィを利用した秘密情報伝送システムの概略を図２に示す．

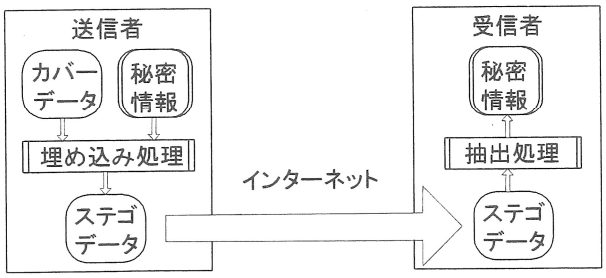

図２　デジタル情報のステガノグラフィ

秘密情報の送信者は画像や音声などの日常ありふれたカバーデータに対して，その内容を人間には識別できない程度に改変することにより，秘密情報を埋め込み伝送する．カバーデータに秘密情報を埋め込んだステゴデータと呼ぶ．受信者は予め取り決められた手順によってステゴデータより秘密情報を復号する．今日のインターネットでは日常会話としての情報が無数にやりとりされているため，秘密情報が隠蔽されている情報を発見すること自体が困難となる．

3.　マルチィメディアデータのステガノグラフィ

3.1　マルチィメディアデータ

本研究で用いるマルチィメディアデータとして，テキストデータ，音声データ，画像データ，動画データについての形式について述べる．

3.1.1　テキスト（バイト）データ

ビットは通常 8 ビット (bit) にまとめられ、"バイト"と呼ばれる．8 ビットで 1 バイト（byte）を表し，文字の基本単位を表す．

各情報の断片は，コンピュータの内部で符号化される．2 進化 10 進法は，現在使用されている符号化システムである．大型コンピュータの拡張 2 進化 10 進コードと小型コンピュータでのアスキーコードは，ほとんど一般的な符号化システムである．日本語データは 2 進数の 16 ビットで符号化される．

3.1.2　音声データ

ステガノグラフィ技術において媒体となる音声データとして wave ファイルを使用した．wave ファイルは Windows 上で扱うことのできる音声データであり，基本的には１つの RIFF(Resource Interchange File Format)チャンクに２つのサブチャンクのある構造をしている．

内容	バイト数	名称	名称
"RIFF"の４文字	4		RIFF ヘッダ
RIFF データサイズ	4		
"WAVE"の４文字	4		RIFF データ
"fmt "の４文字	4	Fmt チャンク	
fmt データのサイズ	4		
fmt データ	---		
"data"の４文字	4	Data チャンク	
data データのサイズ	4		
data データ	---		

図３　RIFF チャンクの構造

チャンクとはデータを構成する単位のことである．PCM フォーマットの WAVE ファイルについて，それぞれのチャンクとその構造について説明する．RIFF チャンクは，別名親チャンクとも呼ばれ，中には fmt・data の２つのチャンク

があり，図3のような構造をしている．ここでは，Dataチャンクのdataデータ部分に秘密データを埋め込む．

図3を見てわかるように，WAVEファイルの先頭には”RIFF”の四文字が格納されており，fmtチャンク，dataチャンクの先頭にもそれぞれ“fmt”と“data”という文字が格納されている．“RIFF”は，このファイルがRIFF形式であることを表しており，“fmt”と”data”はそれぞれのチャンクの位置を表す役割をしている．

3.1.3　画像データ

画像(image)を符号化する場合には，まず画像全体を細かく縦横のます目に分割する．ここで1インチ(2.54cm)あたりいくつのます目に分割するかを解像度と呼ぶ．1つのます目のことをピクセルと呼ぶ．

画像データとしてBMPファイルを使用する．BMPはWindowsで使用する標準的なファイルである．画像を符号化する場合には，まず画像全体を細かく縦横のます目に分割する．1つのます目のことをピクセルと呼ぶ．画像を白黒濃淡画像を表す場合は，1つのピクセルは，まっ白“11111111”から，まっ黒“00000000”までの8ビットの濃淡で表す．

カラー画像の場合には，1つのピクセルの色や明るさを，「赤」「緑」「青」3原色の強さ(分解能)をそれぞれ0～255の段階(つまり8ビット)で表し，1ピクセルについて24ビットを使用する．

3.1.4　動画データ

動画データとしてWindowsの代表的なメディアファイルであるAVIファイルは3.1.2節で述べたRIFF形式となっている（図4参照）．

<table>
<tr><td colspan="4">LIST (hdrl)チャンク</td></tr>
<tr><td rowspan="9"></td><td>(Avih)</td><td colspan="2">MainAVIHeader構造体</td></tr>
<tr><td rowspan="3">List
(strl)</td><td>(strh)</td><td>ビデオデータ用構造体</td></tr>
<tr><td>(strf)</td><td>BITMAPINFO構造体</td></tr>
<tr><td>(strn)</td><td>オプションデータ</td></tr>
<tr><td rowspan="3">List
(strl)</td><td>(strh)</td><td>オーディオデータ用構造体</td></tr>
<tr><td>(strf)</td><td>WAVEFORMAT構造体</td></tr>
<tr><td>(strn)</td><td>オプションデータ</td></tr>
<tr><td>(ISFT)</td><td colspan="2">ソフトウェア情報</td></tr>
<tr><td>(IDIT)</td><td colspan="2">作成日</td></tr>
<tr><td colspan="4">(JUNK)　2048バイトにするダミーサブチャンク</td></tr>
<tr><td colspan="4">LIST (movi)チャンク</td></tr>
<tr><td rowspan="5"></td><td>(00db)</td><td colspan="2">DIBデータ</td></tr>
<tr><td>(JUNK)</td><td colspan="2">ビデオデータ用構造体</td></tr>
<tr><td colspan="3">…</td></tr>
<tr><td>(00wb)</td><td colspan="2">WAVEデータ</td></tr>
<tr><td>(JUNK)</td><td colspan="2">オーディオデータ用構造体</td></tr>
<tr><td colspan="4">(idxl)　再生順を指示するサブチャンク</td></tr>
</table>

図4　RIFF-AVI フォーマット

AVIファイルとはオーディオ，ビデオを交互に配置したファイルという意味で，ヘッダ情報を保存するチャンクや，ビデオフレーム“db”・オーディオデータ“wb”のある“movi”チャンクから構成される．

動画データの最小単位は「画像フレーム」と呼ばれる静止画像データである．動画データは，その画像データを連続して出力したもので，通常1秒間に30枚程度である．

3.2　マルティメディアへのステガノグラフィ

3.2.1　テキストデータへのステガノグラフィ

テキストメディアへのステガノグラフィとは，テキスト文章の字面情報に対して秘密情報信号を埋め込んで秘匿する手法である．

表2に示すような簡単な方法がある．
メッセージ原文であるダミーデータの下線部分に秘密情報を隠す方法について説明する．

表2　テキストメディアへのステガノグラフィ

テキスト原文
コンピュータ 分野の一つである人工知能とは，コンピュータに人間のように知的な 機能 を 実現することが目的です．
秘密情報を埋め込んだテキスト
コンピュータ 分野の一つであるＡＩとは，計算機に人間のように知能を持った 振る舞い を 持たせることが目的です．

表3に示すように，それぞれの文字の原型に関して派生形を考えたコード表を準備する．テキスト原文にコード表を用いて，原型を使用している文字があれば0を，派生形を使用している文字があれば1とする．

表3　文字列変換コード表

原形(0)	派生形(1)
コンピュータ	計算機
分野	領域
人工知能	ＡＩ
人間	人
知的な	知能を持った
機能	振る舞い
実現する	持たせる

このようなアルゴリズムで，表3に示すように，それぞれの原型に関して派生形コード表を用いて，テキスト原文に元のテキスト内容の意味を変えずに秘密情報である半角1文字を示す“00110111”を隠すことができる．秘密を埋め込んだテキストは，テキスト原文の下線部分の文字列の選択を0，0，1，1，0，1，1，1とし，8ビットの情報である半角1バイトの情報が，隠蔽できる．

テキストのメッセージの送信者と受信者が，このような秘密の文字列変換コード表を共用することによりテキストメディアへのステガノグラフィを実現できる．この原理は非常に簡単であるが，秘密情報のデータ量が非常に少なく，テキストのメッセージ文が不自然になりやすい．

3.2.2　音声メディアへのステガノグラフィ

音声メディアへのステガノグラフィとは，音声信号に対して秘密情報信号を埋め込んで秘匿する手法である．埋め込みによって音声は変化するが，その変化は人間に認識できない程度とする．秘密情報を含む音声が第三者に流出しても，日常やりとりする音声，よく聞く音声であれば，秘密情報の存在自体を察知されず安全であるといえる．また，音声メディアはテキストデータなどと比較してファイルサイズが一般に大きく，また再生時間に比例して大きくなる性質を持つため，容量の多い秘密情報を埋め込む目的に適している．

音声を媒体としたステガノグラフィの研究について，現在までに研究が行われているものとして以下のようなものがある．下位ビットコーディングは，一般に，アナログ音声信号をデジタル化する際には，データの量子化が行われる．その情報の下位ビットデータをバイナリで表現した秘匿データに置換する手法である．位相コーディングは，元の音声データを複数ブロック化し，最初のブロックの位置情報を秘匿情報に置き換えることによってデータ埋め込みを行う方法である．スペクトラム拡散コーディングは，DSSS(Direct Sequence Spread Spectrum)と呼ばれる方式を使用した秘匿データ埋め込み方法であり，秘匿データにチップと呼ばれる既知の擬似ランダム信号を掛け合わせることにより，多様な周波数スペクトラムに拡散させ，それを加算ノイズとして音声信号に付加するものである．しかし，これらの方法では秘密データの容量が少ない．

そこで本研究では，音声データを媒体したステガノグラフィに関する研究を行い，その有用性を考えていくことにする．音声データに情報を埋め込む場合に重要なのは，埋め込む場所である．画像の場合と同様に，一目で秘密情報が埋め込まれていることがわかってしまっては意味がない．できるだけ元のデータの内容を変化させずになるべく埋め込み容量を大きくできるかが必要となってくる．そこで，本研究では音声データを用いたステガノグラフィ・プログラムを作成することにより，効率的かつ一般ユーザが手軽に使用することのできる秘密情報非可視化技術を実現することを目的とする．

デジタル音声メディアの保存形式には音楽 CD などに用いられている非圧縮形式（リニア PCM など）と携帯型再生装置に用いられる圧縮形式（mp3 など）がある．本論文では大容量情報の秘匿を目的とするため，データに冗長性を多く持つ非圧縮形式の音声を用いる．圧縮形式への秘密情報秘匿は，音声の冗長性を除去することで圧縮を行っているため，音声を変化させることによる秘密情報秘匿手法では大容量情報の秘匿は難しい．

非圧縮形式の WAVE ファイルには実際の音声データが格納されている．データの表現は 8bit と 16bit の場合で表現方法が異なり，8bit の場合は 0～256 までの符号なしの数値，16bit の場合は-32768～32767 までの符号付きの数値で表現される．　データの格納のされ方は，モノラルの場合は図 3 の data データの部分に単純にデータが順次並んでおり，ステレオの場合は左側のデータと右側のデータが交互にならんでいる．

3.2.2.1　最下位ビット置換法

下位ビットコーディングの中でも，埋め込みに使用するビットを最下位ビットのみに限定した手法である．これにより，埋め込み前後の音の変化を最小限に抑えることが可能となる．

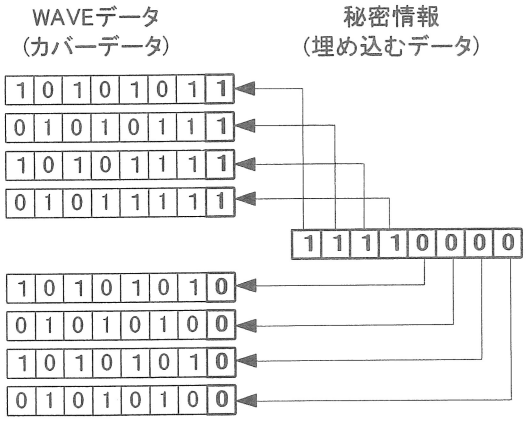

図 5　最下位ビット置換法の原理

また，最下位ビットのみを使用するため，埋め込み可能容量（WAVE ファイルのデータのうち埋め込みに使用できる部分の割合を示す値）は 8 分の 1 つまり 12.5%となる．

図 5 に，最下位ビット置換法を用いて WAVE データに秘密情報を埋め込む様子を示す．WAVE データ，埋め込むデータを共に 2 進数で表現し，埋め込むデータを順に WAVE データの最下位ビットと置換する．

3.3　画像データへのステガノグラフィ

画像メディアへのステガノグラフィとは，画像データに対して秘密情報信号を埋め込んで秘匿する手法である．多値画像は 3.1.3 節で述べたように，それぞれの画像の明るさや色の情報を，複数のビットで記述する．カラー画像の場合だと R(赤)，G(緑)，B(青)の各成分の強さを 8 ビットで表現する．ここでは，そのような形式での画像データの第 1 ビット目を最上位ビット（MSB)，第 8 ビット目を最下位ビット（LSB）として扱う．白黒濃淡画像やカラー画像の最下位ビット部分は画像全体への視覚的影響が少ない．この部分を別のデータに置き換

えても変化が少ない．このことを利用して，最下位ビットに秘密情報を埋め込んでも，視覚的な埋め込みの痕跡が残らずに，秘密データを隠すことができる．この最下位ビットに埋め込む方法は，典型的なステガノグラフィとして知られている．

この方式で埋め込まれるデータ量は，ダミー画像ファイルサイズの 1/8(12.5%) を超えることは無い．最下位ビットだけではなく，その次のビットに埋め込んでも画質が低下しない場合があり，そのような場合の埋め込み容量はカバーデータの 1/4 程度になるが，このように定まった部分にこのように定まった部分に情報を埋め込む場合には攻撃者の対象になりやすく，解読されやすい．

3.4 動画メディアへのステガノグラフィ

動画メディアへのステガノグラフィとは，動画の画像データと音声信号に対して秘密情報信号を埋め込んで秘匿する手法である．

カバーデータに秘密データが隠せる場合，まず秘密データに暗号化または圧縮処理を行う．それからカバーデータのストリームチャンクの中の JUNK や **wb や **dc に暗号化・圧縮の操作を施した秘密データのサイズを 32 ビットで埋め込み、ファイル本体等を埋め込む．その際ビデオ領域ではフレーム画像を RGB それぞれ 8 ビットのプレーン構造に分割した場合，の LSB 部分のプレーンに情報を埋め込む． LSB 部分のプレーン画像では元画像の情報をあまりもたないという特性があるのでそれを利用し情報を隠す．オーディオ領域では小さい音の部分ではノイズが発生してしまうので埋め込みを行わず，大きい音のところに大きさによって 1 ビットあるいは 2 ビットと埋め込むビット数を可変式に変えていく埋め込みアルゴリズムを用いて情報を隠す．ステゴデータから秘密データを抽出する場合，まず 32 ビットのファイルサイズの情報を読み込んでファイルサイズ分の読み込み処理を繰り返す．基本的に埋め込み処理と逆の処理を行う．

3.5 その他の方法

画像データや音声データは，周波数成分に変換して扱うことができる．特定の周波数帯域を秘密情報と置き換えるなど各種手法が提案されている．

4. 実験

4.1 実験方法

3.2.2 節で説明した下位ビット置換法による実験を行う．主観的評価法と客観的評価法の二種類の評価法を用いて，埋め込み率と隠蔽性の関連，またそれぞれの評価法の有効性について調べる．

4.1.1 主観的評価法

主観的評価法とは，埋め込み処理された数秒の音声データ（ステゴデータ）を実際に試聴し，音声データに変化が感じられるかを調べるものである．

実験を行う準備として表4 に示す音声ファイルを用意して，それぞれに 0bit（埋め込み無し），4bit，8bit，10bit，12bit，14bit の埋め込みを行う．

まず被験者に埋め込み前の音声を試聴させる．次に埋め込み後の音声を無作為な順番で試聴させる．そして6種類の音声ファイルのうち，どのファイルに埋め込みがなされていると判別できるかを検証する．被験者にはいくつのファイルに埋め込みがなされているか等の情報は一切与えない．

秘密データにはカバーファイルの全域にわたって埋め込めると予測されるファイルサイズを持った画像ファイルや，動画ファイルを無作為に選んで使用する．

表4　実験条件

(a)カバーファイル

	内容	再生時間(分:秒)	ファイルサイズ(byte)
音楽A	ロック	00:11	1,048,044
音楽B	クラシック	00:10	933,932

(b)WAVEファイル形式(音楽A，音楽B共通)

フォーマット形式	リニアPCM
サンプリングレート	44.1kHz　(sample/sec)
量子化ビット数	16bit　(bit/sample)
チャンネル	モノラル

(c)秘密データファイルサイズ(共通)単位 (Kbyte)

0bit	4bit	8bit	10bit	12bit	14bit
0	233	466	583	699	816

4.1.2 客観的評価法

客観的評価法とは，埋め込みによる音声の変化を，ある計算式によって数値で評価する方法である．本研究では信号の劣化度合いの尺度として一般的に用いられている PSNR (Peak Signal to Noise Ratio：ピーク信号対雑音比) による評価を行う．

PSNRとは，元の音声と埋め込み後の音声の間にどれだけ差があるかを表す評価指標となる数値であり，単位はデシベル[dB]で表される．

ノイズの混入が増えるとPSNRは減少し，逆にノイズの混入が全くなければ PSNR は無限大(∞)となる．本研究ではPSNRの値を式下記のように定義する．

$$PSNR\left[dB\right]=20\log_{10}\left(\frac{MAXVAL}{\sqrt{\frac{1}{N}\sum_{k=1}^{N}\left(f\left[k\right]-f'\left[k\right]\right)^{2}}}\right)$$

$MAXVAL$：$f[k]$ の取りうる最大値(量子化ビット数16bitの時 2^{16} となる)
N：サンプル数
$f[k]$：埋め込み前のサンプル値
$f'[k]$：埋め込んだ後のサンプル値

本研究ではPSNRを計算するプログラムを開発し，主観的評価法で用いた12個の音楽ファイルについてPSNRを計算する．また，埋め込み前と埋め込み後の波形の変化についても比較検討する．

4.3　実験結果

今回行った主観的評価法と客観的評価法の実験結果を示し，それぞれ考察を行う．

4.3.1 主観的評価法

主観的評価法により，被験者約 60 人のうち，音声ファイルに埋め込みがされていると判断した割合をまとめたものを結果として表5に示す．また，参考にカバーデータに対するみ秘密データの埋め込み率も表示する．

表5　主観的評価法による実験結果

埋め込みビット数	0bit	4bit	8bit	10bit	12bit	14bit
埋め込み率	0%	25%	50%	62.5%	75%	87.5%
ロック	8%	10%	30%	58%	100%	100%
クラシック	12%	15%	67%	87%	100%	100%

4.3.2 客観的評価法

埋め込みされたWAVE ファイル各々に対して，元データとのPSNR値を計測した値を表にまとめたものを表6 に示す．

表6　埋め込み処理後のPSNR[dB]計測値

埋め込みビット数	0bit	4bit	8bit	10bit	12bit	14bit
ロック	∞	92.1	55.1	43.6	31.4	19.5
クラシック	∞	91.7	54.3	43.0	30.6	17.4

5.　まとめ

本研究はステガノグラフィにおける媒体データにはWAVE ファイルを使用，手法として，下位ビット置換法を採用し，その有効性について研究を行った．その結果より，16 ビット WAVE ファイルにおいて，以下のようなことが確認された．

- 4bit までは完全な隠蔽性を持つ
- 8bit 付近が隠蔽性の限界である
- 14bit 等の高い埋め込み率でも利用価値がある
- PSNR の値だけで隠蔽性を判断することはできない
- 振幅値の大きいカバーファイルが使用に適している

本研究では埋め込み限界容量がカバーファイルの50%程度と，ある程度実用に耐えうると思われる結果が得られた．さらなる埋め込み率向上のためには新たな埋め込みアルゴリズムの考案が必要であると考えられる．

今後は，動画へのステガノグラフィの研究を行うことが必要であると考えられる．

参　考　文　献

[1] Invitation to BPCS-Steganography:
http://www.datahide.com/BPCSj/

(2007年10月12日　受理)