

# デジタル音声への情報ハイディングに関する研究

岩 切 宗 利

## 論 文 の 内 容 の 要 旨

近年のデジタル通信網と情報処理技術の発達は、高速かつ大容量なデータ伝送を可能にした。デジタル社会では、このような広帯域デジタル通信網を利用した情報伝送が不可欠である。ネットワークを利用して、デジタルデータを伝送すると、その再現性の高さから情報の漏洩や盗用、改ざんなどの危険性に常時さらされてくる。

その対策として、暗号を導入すれば、低いコストにより情報の内容を秘匿できる。しかし、この方法では、意図しない第三者による不正な解読の対象になりやすい。たとえば、暗号文を伝送した事実そのものが、有用な情報を与える手掛りになる場合もある。

また、デジタルコピーされたコンテンツが不正に氾濫すると、マルチメディアの著作権侵害という新しい社会問題が発生する。メディアの配信形式として封印や暗号化を用いれば、違法な行為がある程度まで防止できる。しかし、復元されたコンテンツへの不正な行為を防ぐことができない。メディアの市場を拡大する観点からすれば、厳しい利用制限が望ましくない場合もあるであろう。

最近、これらの問題を解消する技術として情報ハイディングが注目をあつめており、その形式や利用形態によって様々に分類されている。一般には、利用者が知覚できないように、マルチメディアの冗長成分やランダムな領域へ情報を紛れ込ませる技術である。本論文では、第1章にデジタル音声を対象とした情報ハイディングの概要を示し、第I部にてステガノグラフィ技術、第II部にて電子透かし技術を提案する。

第I部のステガノグラフィは、情報を読めない形式へ変換する暗号技術と異なり、情報の存在そのものを秘匿する技術である。例えば、デジタル電話を用いた音声通話の際に、秘密のメッセージを伝送符号に埋め込み、特定の受信者のみが情報を抽出できるようにする。不正な第三者は、通信路上の伝送データを観察しても、埋込みの存在すら検知できない。ステガノグラフィは、秘密通信の存在を秘匿できる点が興味深い。

第I部は、8章により構成される。第2章では基本的な圧縮手順である適応量子化PCMによる音声符号への埋込み方式を示す。第3章から第6章では、音声信号をITU-T勧告の国際標準規格に定められた手順を用いて符号化する際に、情報を埋め込む技術について述べる。第7章では、音楽ソフトの品質をほとんど劣化しないスペクトル拡散技術を応用した方式を提案し、第8章では、その秘匿性能をさらに改善できるスクランブル方式を示す。第9章では、楽音符号の標準形式であるSMF (Standard MIDI File)への埋め込み技術を提案し、それを応用した原本性保証の原理について述べる。

第II部の電子透かしは、利用者が知覚できない形式として、著作権等の情報をデジタルコンテン

ツに埋め込み、不正行為の証明に役立つ試みである。ステガノグラフィでは、埋め込まれた情報が重要であるのに対し、電子透かしは埋込み対象のコンテンツそのものに価値がある。そのため、電子透かしでは、コンテンツの品質を損わないことが重要とされる。また、何らかの信号処理により埋込み情報が失われると、電子透かしの目的を達成できないので、攻撃耐性も必要である。これらの品質と保全性に関する考察は、電子透かしを議論する際に不可欠とされている。

第Ⅱ部は、7章により構成されている。第10章では、スペクトル拡散方式の攻撃耐性を高めた電子透かしを提案する。第11章では、直接拡散と異なるスペクトル拡散技術である周波数ホッピングを電子透かしに導入する。第12章では、統計的な電子透かしを周波数領域上に施す差分拡散法について示す。第13章では、2次元に配列した音声データの相互関係を電子透かしの検出に利用する。第14章では、候補鍵の概念を新たに導入した反応検査方式を示す。第15章では、可変型の電子透かしを用いた試聴システムについて述べる。第16章では、SMFを対象とした電子透かし技術を示し、その応用形式として半雑音化の概念を示す。

これらの研究により、様々な形式のデジタル音声データに対し、情報を密かに埋込み可能であることが明らかとなった。その結果、将来のデジタル通信を利用したステガノグラフィおよびマルチメディアコンテンツの著作権保護に用いる電子透かしの開発に有効な指針を得ている。

以上