平成 17 年度

学士学位論文

音声情報分割による秘匿通信

Audio Secret Sharering

1060325　田井 修三

指導教員　福本 昌弘

2006 年 3 月 10 日

高知工科大学 情報システム工学科

要 旨

音声情報分割による秘匿通信

田井 修三

近年，光通信インフラなどの整備が進み，動画や音楽ファイルといった大容量のディジタルコンテンツのやり取りが，誰でも，手軽に行えるようになってきた．そして現在，問題となっているのが，ディジタルコンテンツの違法コピーなどによる著作権管理の問題である．この著作権管理の問題がある中で，不特定多数の人々が混在している中で，その中にいる特定の人々だけに対して音声情報を提供したい, といった要求が考えられる．

本研究では，音が波であることに着目し，波の性質である波の重ね合わせの原理とディジタル信号処理を利用した音声情報分割による秘匿通信の実現について検討を行っている．そして，音声情報分割による音声秘匿通信システムを提案している．また，提案したシステムを用いて，計算機シミュレーションを行った結果，提案した音声秘匿通信システムは，秘匿通信を実現するための仕組みとしてはうまく動作しているが，原信号の再現には問題があることを確認した．

キーワード　音声秘匿通信 重ね合わせの原理 ディジタル信号処理

Abstract

Audio Secret Sharering

Shuzo Tai

In recent years, a communication infra-structure is progress. The activities an exchange of digital contents is done. Now, how to management of a copyright becomes a problem. In management of a copyright becomes a problem, The demand that I want to offer voice information to Specific person when there are many and unspecified people is thought. In this research, I paid attention that the sound is a wave. Then I have examined about Audio Secret Sharering system that the principle of superposition and the digital signal processing were used. I have proposed that Audio Secret Sharering System. And, I have done computer simulation that Audio Secret Sharering system were used. As a result, Audio Secret Sharering System has operates well that the mechanism to materialize a communication hiding. but, there is a problem in reproduction of original signal.

key words Audio Secret Sharering System , The principle of superposition , The digital signal processing

目次

図目次

表目次

第 1 章

序論

1.1 研究の背景と目的

近年，光通信インフラなどの整備が進み, 動画や音楽データといった大容量のディジタルコンテンツのやり取りが，誰でも，手軽に行えるようになってきた．特に，音楽データは，MP3 等のデータ圧縮技術が広く普及したことにより，データのやり取りが，ますます手軽に行えるようになっている．

そして現在，問題となっているのが，ディジタルコンテンツの違法コピーなどによる著作権管理の問題である．特に，ファイル交換ソフトによるディジタルコンテンツのやり取りは，著作権侵害を引き起こす要因の一つとして深刻な問題となっている．

そして，ファイル交換ソフトなどによって，大衆の間に広まった音楽情報などの著作物は，故意の有無に関わらず，公的な場において，無断で使用されている．過去の事例としては，ダンス教室において，ダンス指導の際に音楽を無断使用し，著作権を侵害した事例がある．この事例では，日本音楽著作権協会 (JASRAC) が、ダンス教室と経営者に過去 10 年分の使用料相当額，約 5130 万円の賠償などを求める訴訟が行われた，この訴訟では，最高裁が著作権侵害を認定した．

現在，このようなファイル交換ソフトや違法コピーの問題に対する有効な解決策は存在しない．また，楽曲の著作権所有者は，楽曲が使用される場所や状況をコントロールすることもできない．そこで，著作権所有者側の要求として，不特定多数の人々が混在している中で，その中にいる特定の人々だけに対して音声情報を提供したい, といった要求が考えられる．

このような要求に応えるために，著作物へ対価を支払った人，支払っていない人が混在するような場所において，著作物へ対価を支払った人だけに対して完全な音楽情報を提供できるような仕組みを考える必要がある．

そこで，本研究では，前述した要求に応えることのできる仕組みとして，重ね合わせの原理とディジタル信号処理を利用した音声秘匿通信システムを提案する．そして，計算機シミュレーションを行い，そのシミュレーション結果から，S/N 比を用いて提案した音声秘匿通信システムの評価を行う．

1.2　本論文の概要

第 2 章では，本研究で用いる，ディジタル信号処理についての基礎技術である，ディジタルフィルタと適応信号処理について述べる．

第 3 章では，本研究で用いる，適応フィルタによる信号補正について述べる．

第 4 章では，重ね合わせの原理を利用した，音声秘匿通信システムを提案する，そして，計算機シミュレーションを行い，提案した音声秘匿通信システムの評価を行う．

最後に第 5 章では，本研究の結論を述べ，今後の課題を述べる．

第 2 章

ディジタル信号処理

2.1 まえがき

音声，音楽といった音響信号は連続的な量をもつアナログ信号である．このアナログ信号を離散的な値をもつディジタル信号に変換することで，コンピュータ上でデータの処理を行うことができる．

処理の対象となる観測信号は，何らかのアナログシステムによって生成されたものである．したがって，入力されてから観測されるまでの間のシステムに関する何らかの情報を保持している．また，観測信号には，雑音や干渉などの不要成分も含まれている．そこで，観測信号から目的とする信号成分を抽出する機能を持ったディジタルフィルタについて考える．

フィルタとは，入力にある処理を行い変形することによって，必要とする出力を得るためのものである．ディジタルフィルタは，有限長の応答をもつ FIR(Finite Impulse Response) フィルタと，無限長の応答をもつ IIR(Infinite Impulse Response) に分類される．[1]

本章では，本研究で用いるフィルタが有限長のフィルタであることから，FIR ディジタルフィルタについて述べた後，FIR ディジタルフィルタを用いて未知のパラメータを推定する機能をもつ適応フィルタについての説明を行う.

2.2 ディジタルフィルタ

2.2.1 FIR ディジタルフィルタ

ディジタルシステムでは，個々の信号を一時的に記憶するため，過去の信号を取り出すことが可能である．そこで，図 2.1 のように，z^{-1} を有限個用いたフィルタを考える．

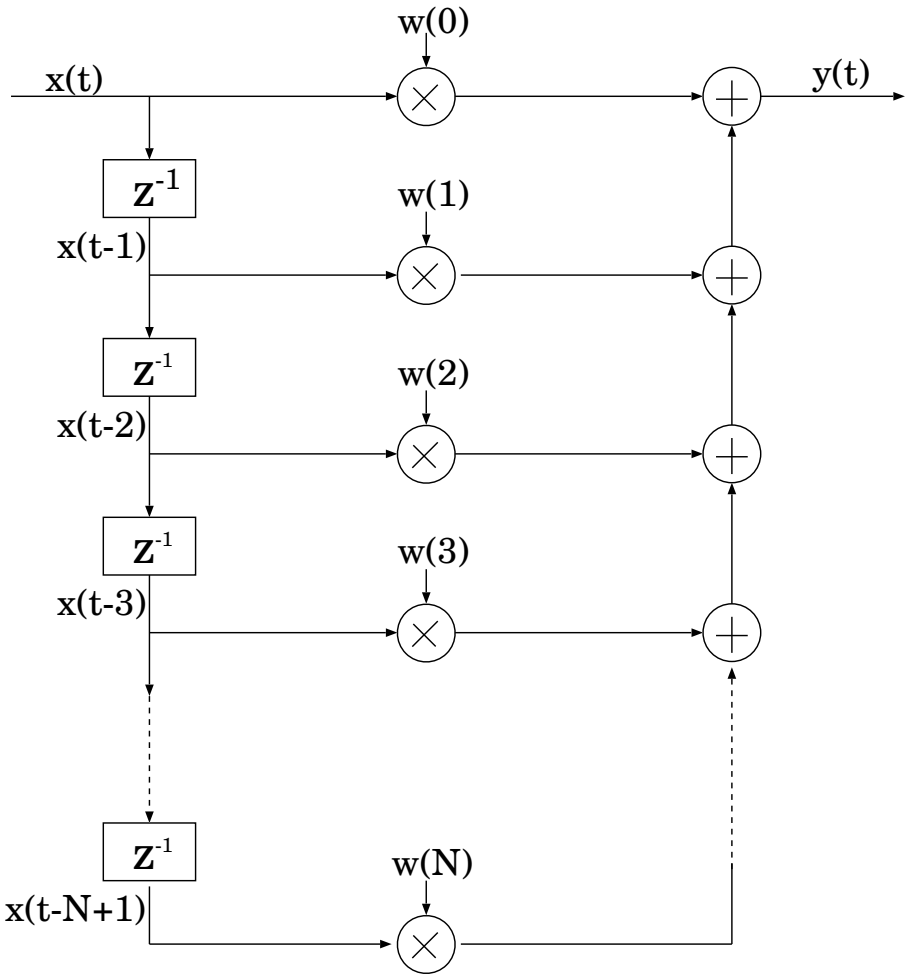

図 2.1 FIR ディジタルフィルタ

図 2.1 では，入力信号 $x(t)$ が各タップにおいてパラメータ (フィルタ係数) と乗ぜられ，それらが加算された結果 $y(t)$ が出力される．このフィルタの入出力関係は，

$$y(t) = \sum_{i=0}^{N-1} w(i)x(t-i+1) \tag{2.1}$$

で与えられる．

このように，インパルス応答の長さが有限長となるようなディジタルフィルタのことを FIR(Finite Impulse Response) ディジタルフィルタと呼ぶ．[1]

式 (2.1) から，出力信号 $y(t)$ はパラメータ w_N に依存することがわかる．このことは，同一の入力信号を与えた場合でもパラメータが異なれば得られる結果も異なることを表している．ただし，パラメータ w_N とは，

$$w_N = [w(0), w(1), ..., w(N)]^T \tag{2.2}$$

で表される．ここで T は転置を表す．

2.3 適応信号処理

信号処理では，観測された信号にフィルタを作用させることによって，望ましい信号が出力されるように処理を行う．このとき，フィルタの特性を決めるパラメータが固定である場合は，時間の変化に関係なく処理を行うことが可能である．しかし，観測信号の統計的性質が時間と共に変化する場合には，固定的な処理では正確に対応できない．そこで，時間と共に変化する信号の性質に応じて，パラメータを更新することのできる適応フィルタを用いる．このような処理を行うために，Widrow の先駆的な研究により始められたのが適応信号処理 [2] である．

近年では，移動通信システムの分野の飛躍的な成長により，適応エコーキャンセラ，適応ノイズキャンセラ，適応干渉キャンセラ，適応等化器などの適応信号処理技術が多く利用されている．[2][3]

2.3.1 適応フィルタ

次に，FIR 形で構成された未知システムのパラメータ (インパルス応答) を推定することを考える．図 2.2 にシステムのブロック図を示す．ただし，図 2.2 における変数についての説明は表 2.1 に示す．

2.3 適応信号処理

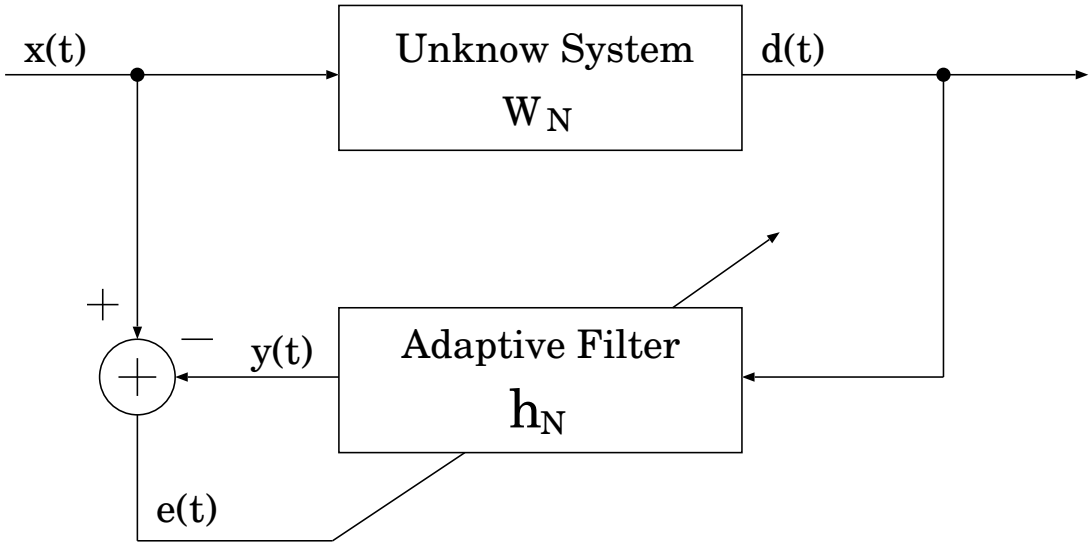

図 2.2　適応フィルタを用いたブロック図

表 2.1　図 2.2 における変数の説明

t	**時刻**
N	**インパルス応答長 (フィルタタップ数)**
$x(t)$	**入力信号**
$w(t)$	**未知システムのフィルタ係数** $(w_N = [w(0), w(1), \cdots, w(N)]^T)$
$h(t)$	**適応フィルタのフィルタ係数** $(h_N = [h(0), h(1), \cdots, h(N)]^T)$
$d(t)$	**未知系の出力信号**
$y(t)$	**推定系 の出力信号**
$e(t)$	**出力誤差**

このとき，未知系出力信号 $d(t)$ と推定系の出力信号 $y(t)$ は

$$d(t) = \sum_{i=0}^{N-1} w(i)x(t-i+1) \tag{2.3}$$

$$y(t) = \sum_{i=0}^{N-1} h(i)x(t-i+1) \tag{2.4}$$

と表すことができる．また出力誤差 $e(t)$ は，

$$e(t) = d(t) - y(t) \tag{2.5}$$

と表される．

式 (2.3)，(2.4) において

$$w(i) = h(i); \ \ \forall_i = 0, 1, \cdots, N-1 \tag{2.6}$$

であれば，常に同じ出力を得ることができる．したがって，未知システムのインパルス応答長が有限で，その個数が既知であるならば，同一の入力信号に対して完全に等しい出力結果を与える FIR ディジタルフィルタを構成することが可能である．

しかし，一般に，未知システムのインパルス応答長は無限に続く．この場合，式 (2.6) のような仮定が成り立たないために，同一の入力信号に対して完全に等しい出力結果が得られるような FIR ディジタルフィルタを構成することはできない．

そこで，室内音響系をはじめとする実際のシステムの多くのインパルス応答が，時間と共に減衰していくという性質を利用する．

すると，未知系システムのインパルス応答のうち最初の適当な N 個の値を推定することによって，推定系出力信号を未知系出力信号に近づけることが可能である．

このようにして，推定システムの出力 $y(t)$ が未知システムの出力 $d(t)$ に近づくように，推定システムのパラメータ h_N を逐次的に推定する学習機能を持ったフィルタのことを，適応フィルタという．[2][3]

2.3.2 適応アルゴリズム

適応アルゴリズムとは，各時刻で観測される入力信号 $x(t)$ と出力誤差 $e(t)$ を用いて，パラメータを修正することによって最適解を求める計算手順のことである．[2] 適応アルゴリズムは，1960 年に Widrow-Hoff の LMS アルゴリズムに始まり，1967 年これとは独立に，野田と南雲により学習同定法が発表された．また，その他にも RLS アルゴリズム，BLMS アルゴリズムなどが挙げられる．図 2.2 において，入力信号 $x(t)$ に対する未知系出力 $y(t)$

は，式 (2.7) のように与えられ．

$$y(t) = \sum_{i=0}^{N-1} h(i)x(t-i+1) \tag{2.7}$$

式 (2.7) で表される $y(t)$ は，入力状態ベクトル $x_N(t)$ および係数ベクトル h_N の内積として

$$y(t) = h_N^T x_N(t) \tag{2.8}$$

と表すことができる．ただし，x_N，h_N はそれぞれ

$$x_N = [x(1), x(2), x(3), \cdots, x(N)]^T \tag{2.9}$$

$$h_N = [h(0), h(1), h(2), \cdots, h(N)]^T \tag{2.10}$$

で定義される．

ここで，誤差の 2 乗平均値を評価量 J として

$$\begin{aligned} J &= E[e^2(t)] \\ &= E[(d(t) - y(t))^2] \\ &= E[(d(t) - h_N^T x_N(t)] \end{aligned} \tag{2.11}$$

とする．ただし，$\mathrm{E}[\cdot]$ は期待値をあらわす．図 2.2 では, 未知系出力 $d(t)$ と推定系出力 $y(t)$ との差の 2 乗平均値が最小となるように, 適応フィルタのパラメータを更新する.

次に, 適応アルゴリズムの基本的なパラメータ更新方法についての手順を示す.

(i) 時刻 $t = 0$ として, パラメータの初期値 h_N を設定する (通常 $h_N = 0$).

(ii) 時刻 t における出力 $y(t)$ と誤差 $e(t)$ を次式により計算する.

$$y(t) = h_N^T x_N(t) \tag{2.12}$$

$$e(t) = d(t) - y(t) \tag{2.13}$$

(iii) $x_N(t)$,$e(t)$ を用いて各種アルゴリズムで修正量 $\Delta h_N(t)$ を計算し, 次式によりパラメータ $h_N(t)$ を修正して $h_N(t+1)$ を得る.

$$h_N(t+1) = h_N(t) + \alpha \cdot \Delta h_N(t) \tag{2.14}$$

ここで,α はパラメータ修正の大きさを制御する量であるステップゲインを表す.

(iv) t の値を 1 つ増やして上記 (ii)，(iii) を繰り返す．ただし，過程 (iii) のステップゲインとは，パラメータの修正量の大きさを制御し，収束速度を決定するものである．例えば，$\alpha = 0$ のとき式 (2.14) は

$$h_N(t+1) = h_N(t) \tag{2.15}$$

となり，まったくパラメータの更新が行われない．

逆に $\alpha = 1$ のとき式 (2.14) は

$$h_N(t+1) = h_N(t) + \Delta h_N(t) \tag{2.16}$$

となり，算出された修正量分だけパラメータの更新を行う．すなわち，$\alpha = 1$ のときが最適であると言える．

しかし，これはシステムが最良状態のときのみ有効で，雑音などの問題が生じることを考慮すると，必ずしも最適であるとは言えない．したがって，システムの状態にとって最適なステップゲインを選択する必要がある．これらの手順のうち，過程 (iii) の具体的な修正量 Δh_N の算出方法が，各種アルゴリズムを特徴づける部分となる．

表 2.2 代表的な適応アルゴリズムの特徴比較

適応アルゴリズム	特徴	演算量
LMS アルゴリズム	安定性がある 有色信号で収束特性が劣化	2N
学習同定法	高速な収束特性 有色信号で収束特性が劣化	3N
RLS アルゴリズム	パラメータが時不変ならば良好に収束 パラメータが変化すると不安定	$2N^2$

代表的な適応アルゴリズムの特徴と，フィルタタップ数が N の場合の演算量を比較すると表 2.2 のようになる．本研究に用いられるフィルタは，適応アルゴリズムとして学習同定法を利用している．よって，学習同定法の説明を行う．

学習同定法

学習同定法は，LMS アルゴリズムとは独立に導かれた適応アルゴリズムである．しかし，別名 NLMS(Normalized-LMS) アルゴリズムと呼ばれ，LMS アルゴリズムのパラメータ修正項をフィルタの状態ベクトルで正規化されたものとみなすことができる．

ある時刻 k において，推定系出力 $y(t)$ が未知系出力 $d(t)$ に等しいとする

$$d(t) = h_N^T x_N(t) \tag{2.17}$$

と表すことができる．

しかし，$h_N = w_N$ を満たすためには，すべての入力信号 x(t) に対して式 (2.17) が成り立たなければならない．そこで，式 (2.17) を満たす解集合の代表ベクトルを $h_N(t)$ とする．この解集合は，式 (2.17) より，入力ベクトル $x_N(t)$ に直交しているといえる．更に，w_N はこの解集合に含まれているので，$h_N(t)$ はある点から $x_N(t)$ 方向にパラメータ修正したとき，もっとも w_N に近い点といえる．したがって，$h_N(t)$ を $w_N(t)$ に更に近づけるためには，適当に定めた，ある点よりも w_N により近い $h_N(t+1)$ を次の修正パラメータの初期値とすれば良い．

以上のことより

$$\begin{aligned} h_N(t+1) &= h_N(t) + (h_N(t+1) - h_N(t)) \\ &= h_N(t) + \frac{(w_N - h_N(t))^T (h_N(t+1) - h_N(t))}{\parallel h_N(t+1) - h_N(t) \parallel} \\ &\quad \cdot \frac{h_N(t+1) - h_N(t)}{\parallel h_N(t+1) - h_N(t) \parallel} \end{aligned} \tag{2.18}$$

となる．但し，$\parallel \cdot \parallel$ はベクトルのユークリッドノルムを表し，要素の 2 乗和の平方根と定義する．また，式 (2.18) において

$$\frac{(w_N - h_N(t))^T (h_N(t+1) - h_N(t))}{\parallel h_N(t+1) - h_N(t) \parallel}$$

はパラメータの修正量を示し

$$\frac{h_N(t+1) - h_N(t)}{\parallel h_N(t+1) - h_N(t) \parallel}$$

はパラメータの修正方向を示す．

ここで

$$\frac{h_N(t+1)-h_N(t)}{\parallel h_N(t+1)-h_N(t) \parallel} = \frac{x_N(t)}{\parallel x_N(t) \parallel} \tag{2.19}$$

$$\begin{aligned}(w_N - h_N(t))^T x_N(t) &= d(t) - y(t) \\ &= e(t)\end{aligned} \tag{2.20}$$

が成立するので，式 (2.18) は、

$$h_N(t+1) = h_N(t) + \frac{x_N(t)}{\parallel x_N(t) \parallel^2} e(t) \tag{2.21}$$

と変形できる．

学習同定法は，式 (2.21) の修正ベクトルにステップゲインを掛け

$$h_N(t+1) = h_N(t) + \alpha \frac{x_N(t)}{\parallel x_N(t) \parallel^2} e(t) \tag{2.22}$$

で与えられる．

2.4 まとめ

本章では，FIR ディジタルフィルタ，適応フィルタ，適応アルゴリズムなどのディジタル信号について述べた．

また，本研究で用いられるフィルタに利用されている学習同定法という適応アルゴリズムについて述べた．ここでは，ステップゲイン α の役割についても述べている．

第 3 章

適応フィルタによる信号補正

3.1　まえがき

スピーカを用いた音場再生では，スピーカから出力されたそれぞれの音声信号が受ける伝達特性の影響を除去しなければならない．信号補正におけるパラメータ更新過程は

- 伝達特性の逆特性の算出
- 補正フィルタのパラメータ更新

の 2 つに分けられる．伝達特性の逆特性は，適応フィルタを用いて算出する．そして，入力信号を補正するために，スピーカから出力されたそれぞれの音声信号が受ける信号伝達特性 $G_j(x)$ の逆特性を用いて補正フィルタのパラメータを更新する．

3.2　最適な補正フィルタ

図 3.1 は，スピーカを用いた音場再現のためのシステムのブロック図である．ただし，図 3.1 では 1 つのスピーカに対する処理についてのみ示す．システムへの入力信号 $x(t)$ は所望

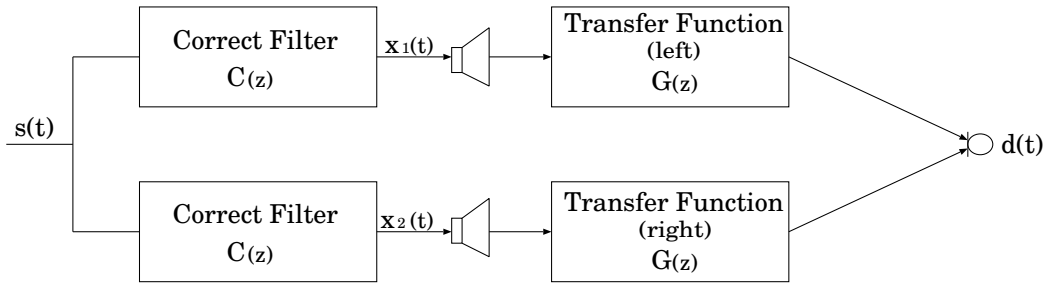

図 3.1　スピーカを用いた音場再現のためのシステムのブロック図

3.2 最適な補正フィルタ

信号 $s(t)$ が補正フィルタ $C(z)$ を通過したものとして与える．また，観測信号 $d_j(t)$ は，入力信号 $x(t)$ が空間の伝達特性 $G_j(z)$ の影響を受けることにより得られる．ここで，システムが線形系であると仮定すると

$$X(z) = C(z)S(z) \tag{3.1}$$

$$D_j(z) = G_j(z)X(z) \tag{3.2}$$

となる．ただし

$$j = \begin{cases} 1 & \text{left} \\ 2 & \text{right} \end{cases} \tag{3.3}$$

とする．また，$S(z)$, $X(z)$, $Dj(z)$ は z 変換後の所望信号，入力信号，観測信号をそれぞれ表す．したがって，所望信号と観測信号の関係は式 (3.1) と式 (3.2) より

$$D_j(z) = G_j(z)C(z)S(z) \tag{3.4}$$

図 3.2 室内伝達特性の逆特性算出のためのブロック図となる．式 (3.4) より所望信号を観測

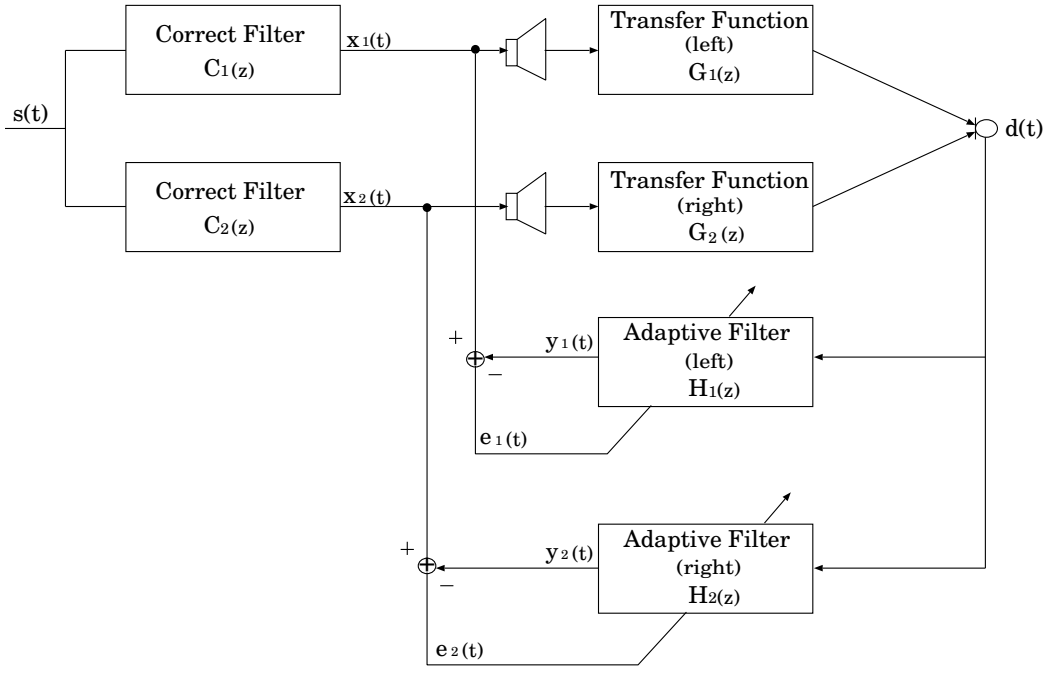

図 3.2　伝達特性の逆特性算出のためのブロック図

信号として得るためには

$$C(z) = G_j^{-1}(z) \tag{3.5}$$

の関係をもつ補正フィルタを構成する必要がある．

3.3　伝達特性の逆特性

図 3.2 伝達特性の逆特性を求めるためのブロック図を示す．適応フィルタ通過後の観測信号を出力信号 $y_j(t)$ とする．出力信号 $y_j(t)$ と入力信号 $x(t)$ の差を出力誤差

$$e_j(t) = y_j(t) - x(t) \tag{3.6}$$

とする．そして，出力誤差が最小となるように学習同定法により適応フィルタのパラメータを

$$h_{jN}(t+1) = h_{jN}(t) + \alpha \frac{d_N(t)}{\| d_N(t) \|^2} e_j(t) \tag{3.7}$$

で更新する．ここで，$d_N(t)$, $h_{jN}(t)$ はそれぞれ観測信号の状態ベクトル，適応フィルタのパラメータであり，$\| \cdot \|$ はベクトルのユークリッドノルムを表す．また，N はインパルス応答長，α はステップゲインを示す．伝達特性の逆特性は，出力誤差が最小となるように適応フィルタのパラメータを更新することで求めることができる．

3.4　補正フィルタパラメータの更新

補正フィルタのパラメータは，3.3 節で求められる適応フィルタのパラメータから求める．

3.2 節では，補正フィルタ C が伝達特性 G_j に対する逆システムと同様の性質である場合に，受聴点での所望信号の再現が可能であると述べた．したがって，複数の経路の伝達特性を補正する場合，3.3 節で示した方法を用いて各伝達特性に対する逆特性のパラメータ推定を行った後，補正フィルタのパラメータが与えられた時，特定の伝達特性のみを補正するように動作しなくてはならない．

そこで，補正フィルタのパラメータが他方の伝達経路の影響を大きく受けた場合でも自らの伝達経路の逆特性のパラメータを算出できるようにする．また，補正フィルタを構成する場合，補正フィルタのパラメータが急激に更新されないように注意しなければならない．なぜなら，急な補正フィルタのパラメータの変化は．観測信号にも影響を及ぼすからである．

したがって，各々の伝達特性に対する補正フィルタのパラメータ修正量を

$$c_{jN}(t+1) = rc_{jN}(t) + (1-r)h_{jN}(t) \tag{3.8}$$

で求める．式 (3.8) では，修正率 $r(0 \leq r \leq 1)$ により式 (3.7) で得られたパラメータをどの程度，適応させるかを決定している．また，補正フィルタのパラメータ生成のためには，過去に得られた補正フィルタのパラメータ値と式 (3.8) で求められた修正量との平均値を

$$c_N(t+1) = \frac{c_N(t) + c_{1N}(t+1) + c_{2N}(t+1)}{3} \tag{3.9}$$

で求める．補正フィルタのパラメータに，過去の値と左右における修正量との平均値を与えることで信号の変動を平滑化する．

本研究で用いた補正フィルタのパラメータ更新過程をまとめると

- 出力誤差 $e_j(t)$ の算出
- 適応フィルタのパラメータ更新

$$h_{jN}(t+1) = h_{jN}(t) + \alpha \frac{d_{jN}(t)}{\| d_{jN}(t) \|^2} e_j(t) \tag{3.10}$$

- 修正量の算出

$$c_{jN}(t+1) = rc_{jN}(t) + (1-r)h_{jN}(t) \tag{3.11}$$

- 補正フィルタパラメータの更新

$$c_N(t+1) = \frac{c_N(t) + c_{1N}(t+1) + c_{2N}(t+1)}{3} \tag{3.12}$$

となる．ここで，$c_{jN}(t)$，$c_N(t)$ はそれぞれ左右における修正量，補正フィルタのパラメータを示す．

3.5 まとめ

本章では，多入力信号補正における最適な補正フィルタの条件とその導出法について示し，複数経路に対する制御を単一の制御系で行う場合のうち，1 つの補正フィルタによって 2 つの異なる伝達特性を補正する多入力信号補正法について述べた．

第 4 章

音声秘匿通信システム

4.1 まえがき

通信インフラなどの整備が進み，動画や音楽ファイルといった大容量のディジタルコンテンツのやり取りが，誰でも，手軽に行えるようになってきた. そして，現在，著作権をどのように管理していくかといったことが問題となっている．この著作権管理の問題がある中で，不特定多数の人々が混在している中で，その中にいる特定の人々だけに対して音声情報を提供したい, といった要求が考えられる．この要求に応えるために，本章では重ね合わせの原理を利用した音声秘匿通信システムを提案する．また，計算機シミュレーションを行い，提案した音声秘匿通信システムの評価を行う．

4.2 音声秘匿通信システム

重ね合わせの原理を利用した音声秘匿通信システムは，音声信号を分割して送ることによって，通信時の秘匿性を確保する．そして，ある受聴点でのみ，元の音声情報を得ることができる秘匿通信システムである．

提案する音声秘匿通信システムの構成を図 4.1 に示す．

図 4.1 を用いながら, 提案する音声秘匿通信システムの説明を行う．提案する音声秘匿通信システムでは，秘匿したい音声情報を分割する．ここでは，2 分割した場合について説明する．

まず，秘匿したい音声情報 $x(t)$ を 2 つの音声信号 $x_1(t), x_2(t)$ に分割する．ここで，音

声信号を分割する理由は，分割した信号に元の信号の情報が全て含まれないようにすることによって，秘匿性を高めるためである．音声信号を分割する条件は，分割した信号同士 $x_1(t), x_2(t)$ を重ね合わせることによって，元の音声情報 $x(t)$ に戻るように分割する．ここで，分割したそれぞれの信号に，互いに逆位相の関係にあるノイズ信号を加える．これも，秘匿性を高めることを目的としている．

そして，分割したそれぞれの音声信号を別々のスピーカから出力する．受聴点 Y で分割した信号同士が足し合わさることによって $y(t)$ を得る．しかし，ここで考慮しなければならないのは，スピーカから出力された音声信号は，受聴点 Y に到達するまでの間に伝達特性 G_1, G_2 の影響を受けるということである．そのため，受聴点 Y で分割した信号同士 $x_1(t), x_2(t)$ をただ足し合わせても，元の音声信号 $x(t)$ を復元することはできない．そこで，適応フィルタ H_1, H_2 を用いて，信号の補正を行う．復元された信号 $y(t)$ が元の信号 $x(t)$ に近い信号になるように逆伝達特性を推定することによって，信号の補正を行っている．

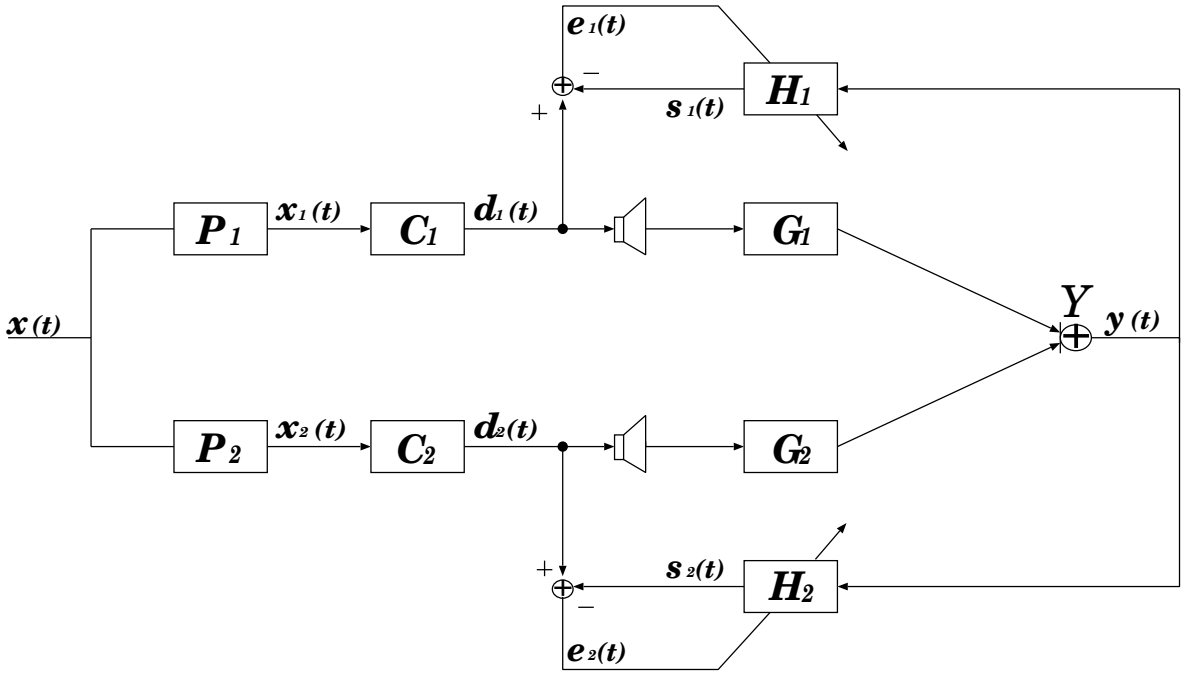

図 4.1　音声秘匿通信システムの構成図

4.3 計算機シミュレーションによる評価

本節では，4.2 節で提案した音声秘匿通信システムの有効性を確認するために計算機シミュレーションを行った．

4.3.1 シミュレーション条件

シミュレーション条件を以下に記す．

- 入力信号 ： 成人男性の声
- 信号の分割方法 ： 低域側の信号 (図 4.3) と高域側の信号 (図 4.4) に 2 分割
- 秘匿方法 ： 分割したそれぞれの信号に互いに逆位相の関係にある白色雑音を加える

また，秘匿信号を分割するにあたって，望ましい分割条件としては以下の 3 点が挙げられる．

1. 足し合わせると，元の信号にもどるように，秘匿信号を分割する．
2. 分割する信号は有限長のものに限る．
3. 分割した信号から，元の信号がわからないように，できるかぎり秘匿性が高くなるように分割する．

ここでのシミュレーションでは，1. と 2. を秘匿信号の分割条件とした．3. についての検討は行っていない．

また，図 4.5 に高域側の信号に白色雑音を加えた信号を，図 4.6 に低域側の信号に白色雑音を加えた信号を，図 4.7 に高域側の信号に影響を与える伝達特性を，図 4.8 に低域側の信号に影響を与える伝達特性をそれぞれ示す．

また，原音に対する再現音の再現精度は，次のような SNR を用いた．

$$SNR[dB] = 10log_{10}\frac{\sum[x_i(t)]^2}{\sum[y_i(t) - x_i(t)]^2} \tag{4.1}$$

ここで，$x_i(t)$ は所望信号の音圧，$y_i(t)$ は観測信号の音圧を表す．元の信号と提案した音声秘匿通信システムからの出力信号との S/N 比を用いて，復元された信号の再現精度の評価を行う．

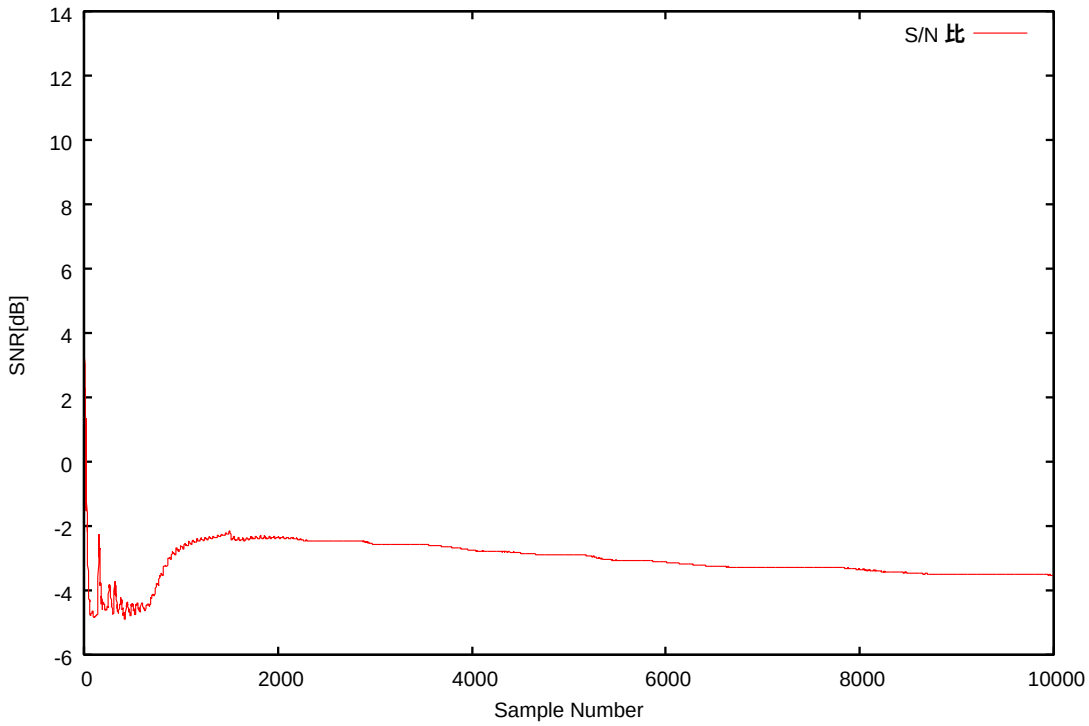

図 4.2　元の信号と復元された信号の S/N 比

4.3.2　シミュレーション結果

4.3.1 節の条件でシミュレーションを行ったときの，元の信号と復元された信号との S/N 比を図 4.2 に示す．元の信号を図 4.9 に，復元された信号を図 4.10 に示す．

元の信号と復元された信号との S/N 比を用いて，復元された信号の再現精度の評価を行った．図 4.2 からわかるように，S/N 比はマイナスの値となっており，復元された信号の再現精度は低いことがわかる．

また，元の信号と復元された信号を実際に聞き比べてみた．実際に聞き比べてみると，元の信号と比べて，復元された信号には少しノイズは残っていて，完全には復元できていないことがわかった．

4.4 まとめ

本章では，波の重ね合わせの原理とディジタル信号処理を利用した音声秘匿通信システムを提案を行った．また，計算機シミュレーションによって，提案した音声秘匿通信システムの評価を行った．このシミュレーションでは，S/N 比を用いて原信号の復元精度の評価を行った．図 4.2 に元の信号と復元された信号との S/N 比を示す．

S/N 比を用いて原信号の復元精度の評価を行った結果，S/N 比はマイナスの値となっており，復元した信号が元の信号に近い信号に復元できていないことがわかった．しかし，元の信号と復元された信号を実際に聞き比べてみると，復元された信号には少しノイズは残ってるものの，元の音声と復元された音声は同じ音声に聞こえた．このことから，完全には復元できていないが，復元された信号の特徴は元の信号の特徴に近い特徴に復元できていると考えられる．元の信号 (図 4.9) と復元された信号 (図 4.10) を比べてみても，見た目には復元された信号は元の信号に近い特徴を持った信号に，復元できていることがわかる．このことから，本研究で提案した音声秘匿通信システムは，秘匿通信を実現するための仕組みとしてはうまく動作しているが，原信号の再現に関しては問題があるといえる．

このシミュレーションで，S/N 比が低くなってしまった原因は，明確にはわかっていない．考えられる原因としては次のようなことが考えられる．まず，本研究では信号の補正を行っているが，適切な信号補正法についての検討は行っていない．そのため信号の補正法に問題があるということが考えられる．そして，秘匿性を確保するために分割した信号に加えるノイズ信号についても検討を行っていない．そのため分割した信号に加えたノイズ信号に問題があったということも考えられる．また，信号の分割方法についても検討を行っていない．そのため秘匿信号の分割に問題があったということも考えられる．その他にも，研究で用いた原信号が，適切でなかったということなども考えられる．

この問題を解決するために今後，次のような検討を行う必要があると考えている．元の信号を復元するための信号補正法についての検討，秘匿信号の分割手法についての検討，分割した信号に加えるノイズ信号についての検討，提案したシステムで用いる原信号について検討を行う必要があると考えられる．

4.4 まとめ

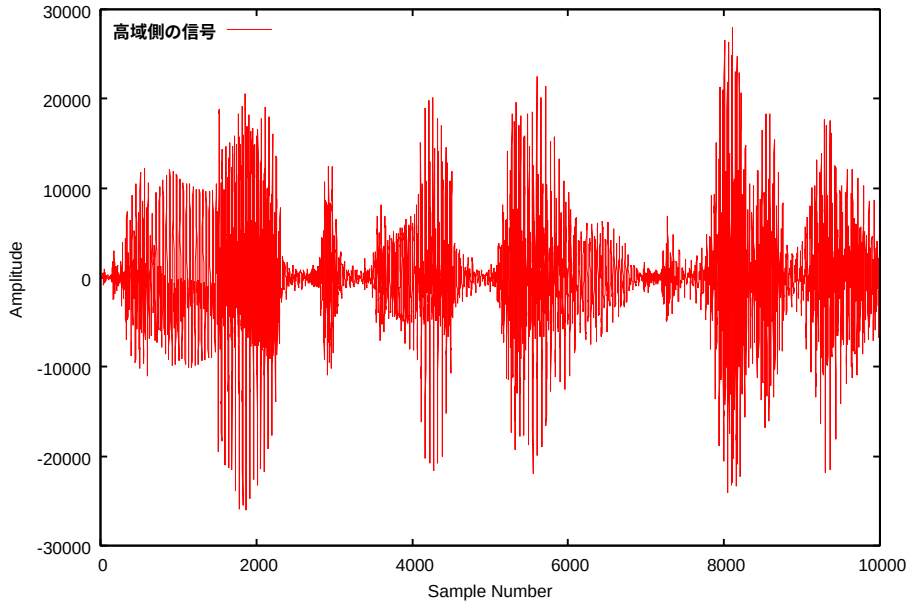

図 4.3　高域側の信号

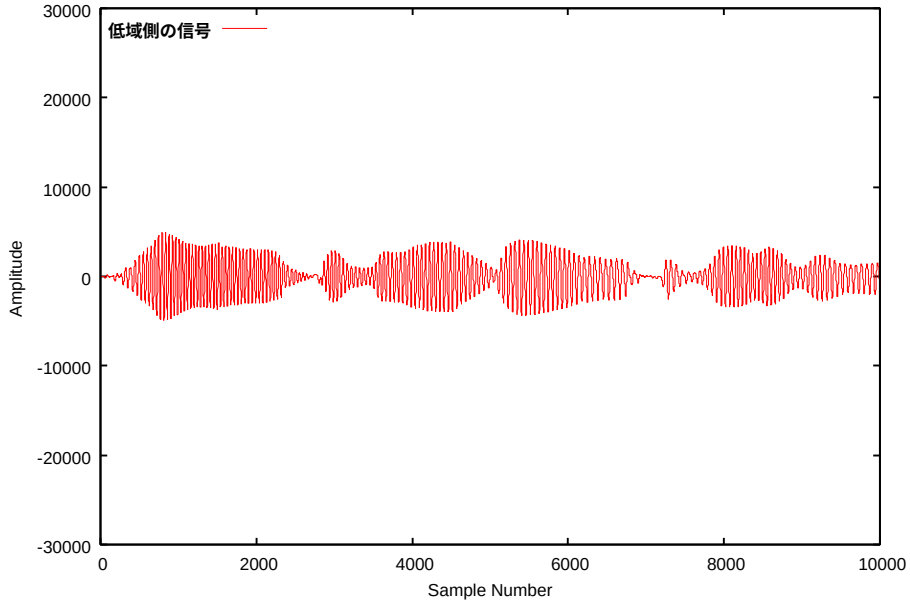

図 4.4　低域側の信号

4.4 まとめ

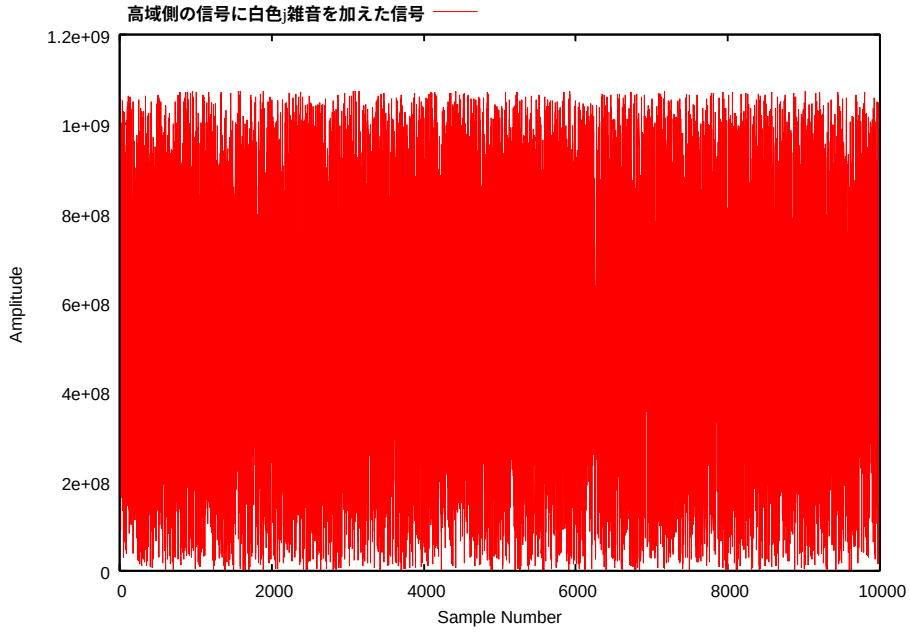

図 4.5　高域側の信号に白色雑音を加えた信号

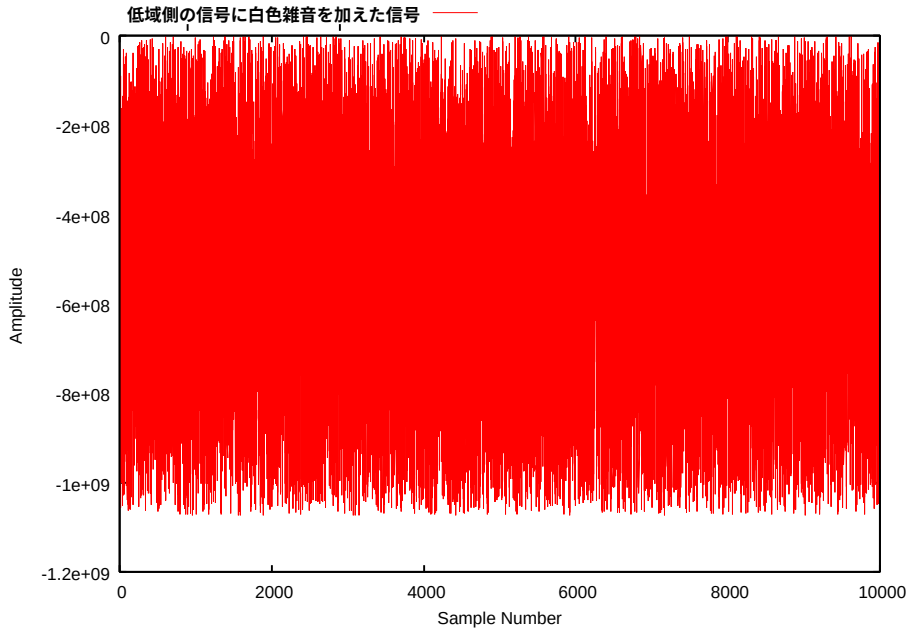

図 4.6　低域側の信号に白色雑音を加えた信号

4.4 まとめ

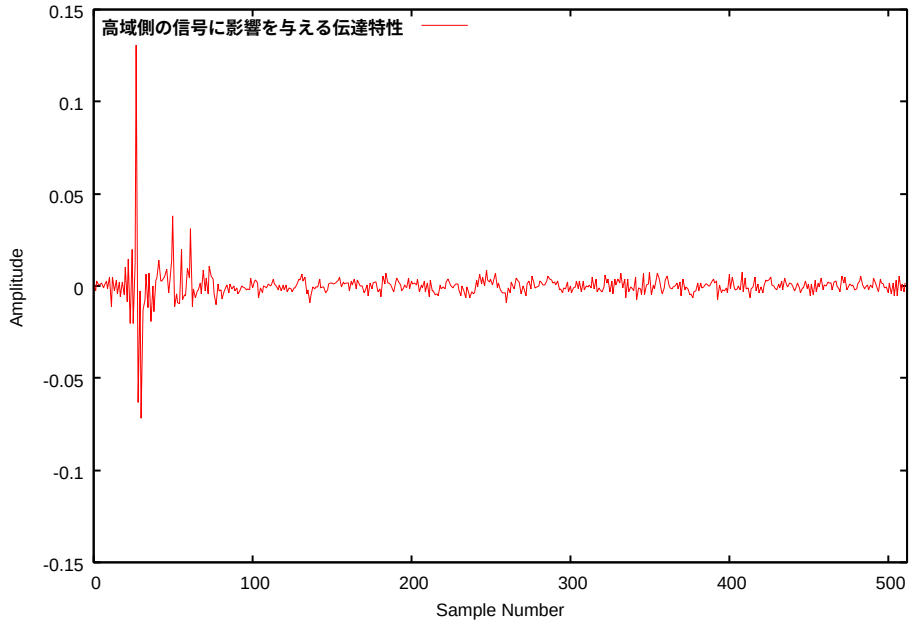

図 4.7　高域側の信号に影響を与える伝達特性

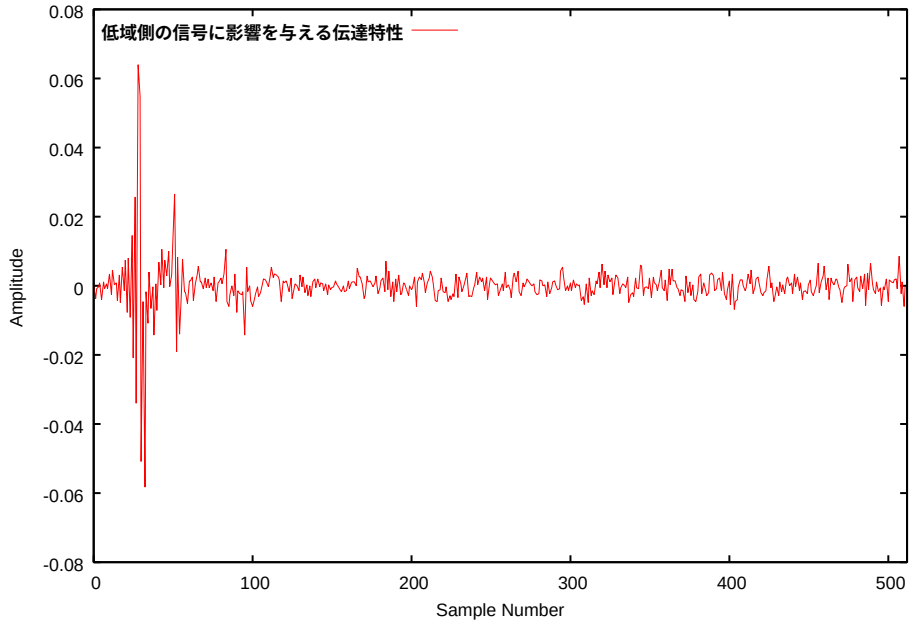

図 4.8　低域側の信号に影響を与える伝達特性

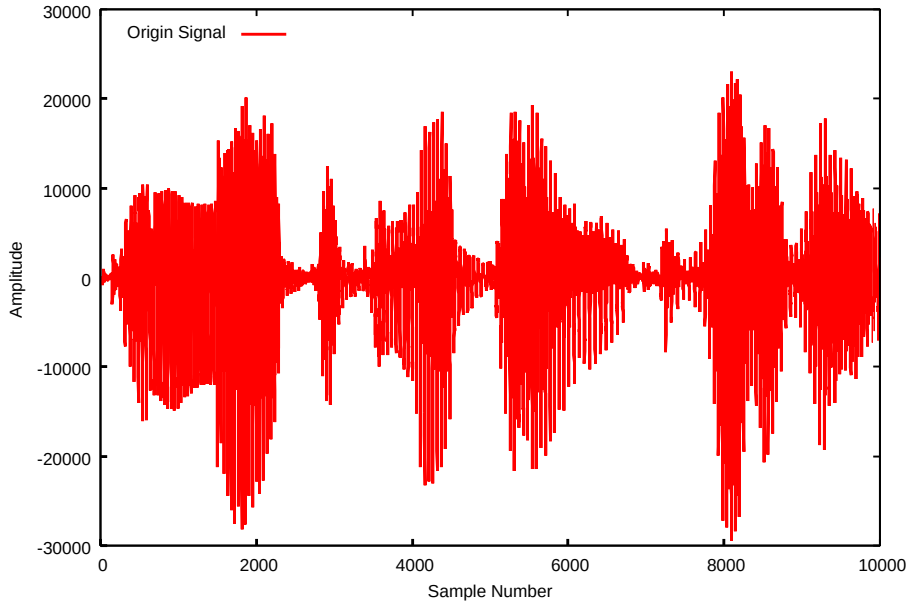

図 4.9　元の信号

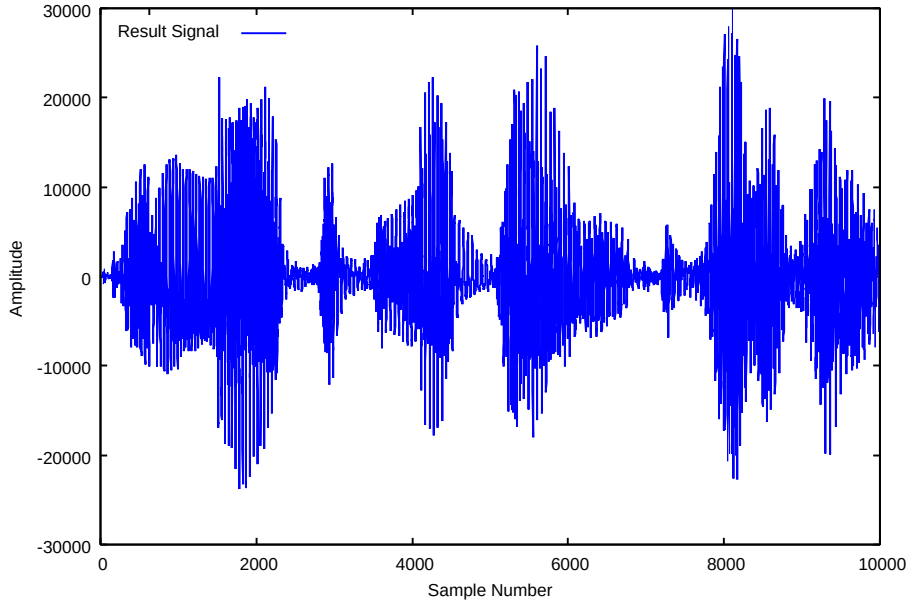

図 4.10　復元された信号

第 5 章

結論

5.1　本研究のまとめ

本論文では，波の重ね合わせの原理を利用した音声秘匿通信システムを提案した．また，提案した音声秘匿通信システムを用いて，計算機シミュレーションを行った．シミュレーションの結果，本研究で提案した音声秘匿通信システムは，秘匿通信を実現するための仕組みとしてはうまく動作しているが，原信号の再現には問題があることがわかった．

5.2　今後の課題

今後の課題としては，秘匿信号の分割手法についての検討や，元の信号を復元するための信号補正法についての検討，信号を秘匿するために用いるノイズ信号についての検討，提案したシステムで用いる原信号についての検討などが必要であると考えている．

また，本研究で提案した秘匿通信システムは重ね合わせの原理を利用しているので，光や無線の電波など，波の性質を持つ媒体を用いた，秘匿通信の実現に応用することができると考えられる．音声以外の媒体での秘匿通信の実現も視野に入れて今後，研究を進めていくことが秘匿通信システムの実現につながると考えられる．

謝辞

卒業研究を完遂するにあたり，福本昌弘先生をはじめ，研究室の方々には大変お世話になりましたので，ここで感謝の辞を述べさせていただきます．

福本昌弘先生には，卒業研究の梗概の〆切前や，卒業研究発表会の前など，夜遅くまで残って御指導して頂き，ありがとうございました．また，私のプレゼンの様子をビデオで撮影して，DVD にして頂き，ありがとうございました．これからは，あの DVD をたまに見ながらがんばっていきます．

また，本研究論文の審議を行って頂いた，島村和典教授と浜村昌則助教授にも，お礼申し上げます．

福本研究室院生の佐伯幸郎さんと清水研究室院生の福富英次さんにも梗概やプレゼンの修正をして頂きありがとうございました．特に，佐伯さんには，呑みに連れて行ってもらったいましたね．かなり楽しかったです．また，ギターを頂き，ありがとうございました．大切に使わせてもらいます．

福本研究室の 6 期生である，下上泰治君，木原崇裕君，三角晃司君，井口貴晶君，高橋一善君にも研究室生活を共に過ごすにあたり，大変お世話になりました．ありがとうございました．

「人生，日々，勉強」という言葉がありますが，この卒業研究を通じて，学んだことは,「人生，日々，研究」であるといことです.「俺は毎日，研究しながら暮らしてるんだ.」と自覚して暮らしている人は少ないと思います．しかし，実は，生きている間は，意識の有無に関わらず，日々，研究活動を行っていると私は思います．日々，起こるさまざまな出来事に対して，どう行動していくかは，研究を行う要領と酷似していると思いました．ということで，これからはさまざまな研究活動をしながら暮らしていこう．そう思っています．では，みなさま，また会う日まで．

参考文献

[1] **辻井重男，鎌田一雄，**“**ディジタル信号処理**”**，昭晃堂，**1997**．**

[2] **辻井重男，久保田一，古川利博，晋輝，**“**適応信号処理**”**, 昭晃堂，**1995**．**

[3] **電子情報通信学会，**“**ディジタルフィルタ信号処理ハンドブック**”**，オーム社，**1993**．**

[4] http : //www.keirinkan.com/kori/kori_physics/kori_physics_1/contents/ph − 1/4 − bu/4 − 1 − 2.htm

[5] http : //impromptu2.hp.infoseek.co.jp/echocanceller.html

[6] **森本 典繁，清水 周一，小出 昭夫，利根川 聡子，**“**データ・ハイディングの開発**”**，日本アイ・ビー・エム最終成果発表論文集，**1998**．**

付録 A

重ね合わせの原理

A.1　まえがき

波の性質を持つ媒体には，重ね合わせの原理が成り立つ．本章では，本研究の重要な要素である，重ね合わせの原理について述べる．

A.2　重ね合わせの原理

重ね合わせの原理とは，2 つ以上の波が同時に存在するとき，実際に観測できる波は，それらの単純な足し算になるということである．一般に 2 つの波 $y_1 = f_1(x,t), y_2 = f_2(x,t)$ が同時に存在するとき実際に観測できる波 y は，それらの単純な代数和

$$y = y_1 + y_2 = f_1(x,t) + f_2(x,t) \tag{A.1}$$

で表される波である. これを，波の重ね合わせの原理という.

この原理が成り立つのは，波動方程式の解が次の性質を持つことと関係がある. すなわち，c_l, c_2 が任意の定数であり，関数 $y_1 = f_1(x,t), y_2 = f_2(x,t)$ がそれぞれ波動方程式の解であるとき，関数 $c_1 y_1 + c_2 y_2$ もまた，その方程式の解である [4].

A.3　逆位相の波同士の重ね合わせ

逆位相の波同士の重ね合わせを行った場合について説明する．図 A.1 の波は，振幅 5 の sin 波である．図 A.2 の波は，振幅 5 の-sin 波である．ここで，図 A.1 の波と図 A.2 の波は互いに逆位相の関係にある．そのため，重ね合わせたると波は互いに打ち消し合い，図 A.3 のように消える．

A.3 逆位相の波同士の重ね合わせ

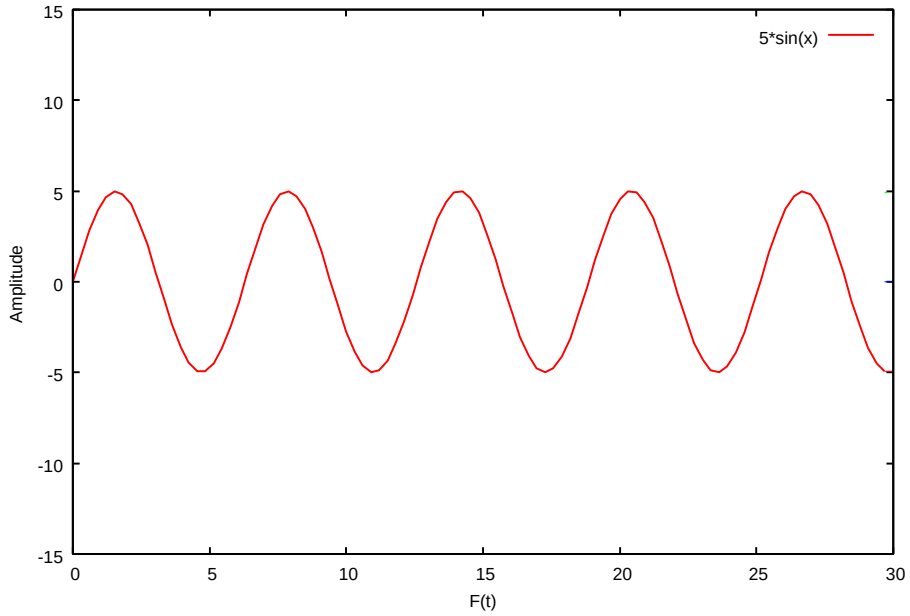

図 A.1　$5 * sin(x)$ **波**

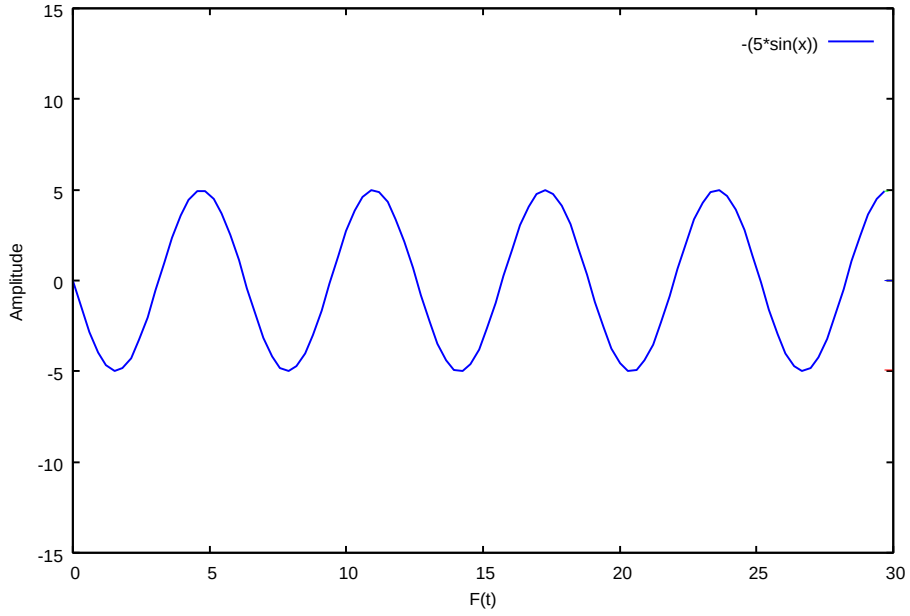

図 A.2　$-(5 * sin(x))$ **波**

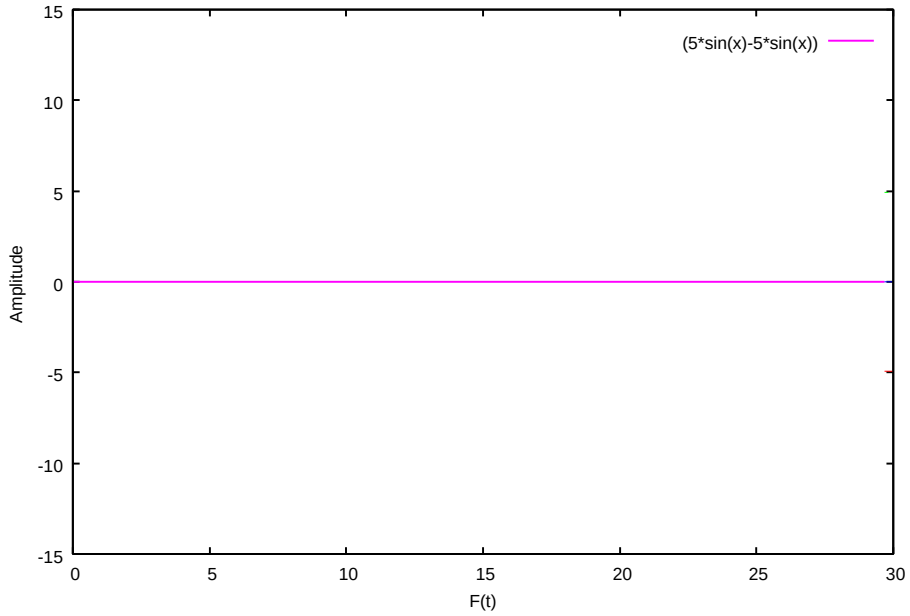

図 A.3　図 A.1 の波と図 A.2 の波を重ね合わせた波

A.4　まとめ

本章では，本研究の重要な要素である重ね合わせの原理について説明した．

また，逆位相の波同士を足し合わせると波は互いに打ち消しあって消える，ということを図を用いて説明した．

付録 B

重ね合わせの原理の応用例

B.1　まえがき

第 4 章で述べた，重ね合わせの原理を利用した音声秘匿通信システムと同じ原理が，エコーキャンセラにも利用されています．

B.2　エコーキャンセラ

エコーキャンセラとは，電気信号や音声の出力が，入力機器に拾われてエコーやハウリングを起こすのを防止する機器や技術のことである．

例えば，電話やテレビ会議等の拡声通話では，スピーカから出力された音がマイクロホンで拾われて話者側に戻ってしまう．結果、戻ってきた音が，不自然で耳障りなエコーとなり，ひどい時にはハウリングが発生してしまう．これら拡声通話に有害なハウリングの発生を防止し，不自然なエコーを除去するためにエコーキャンセラが使用される．

B.2.1　電話回線上での使用例

電話線は 1 つのループした回路です．その上で複数の発信器が信号を流すと、それらの信号をすべて足し合わせた電気信号が回路の上を流れることになります。つまり、DSLAM 側とモデム側で同時に信号を出すと、その信号は電話線の上で一つに混ざってしまうのです。図 B.1 を参照してください。

そこで，電話線上で混ざってしまった信号から所望信号をだけを抽出するといった場合にエコーキャンセラが利用されています．図 B.2 を用いて説明すると，モデムと DSLAM が

B.2　エコーキャンセラ

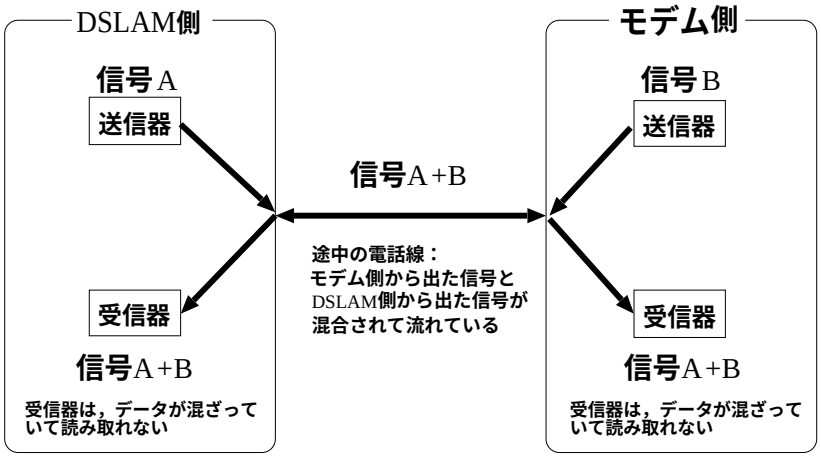

図 B.1　双方がデータを同時に流した場合

同じ周波数を使って信号（DSLAM：「A」，モデム：「B」）を流したとします。すると，電話線の上では両方が混ざった信号（「A ＋ B」）が流れます。このとき、モデム側では、自分の発信器が出した信号（B）を教えてもらうことによって、電話線を流れている混ざった信号（A ＋ B）から引き算すれば、DSLAM が発信した信号（A）を取り出すことができるはずです。要するに、エコーキャンセラは「(A+B)-A=B」という、単純な引き算によって相手の送信した信号を取り出す働きをしています。[5]

このように，第 4 章で述べた，重ね合わせの原理を利用した音声秘匿通信システムと同じ原理が，エコーキャンセラにも利用されています．

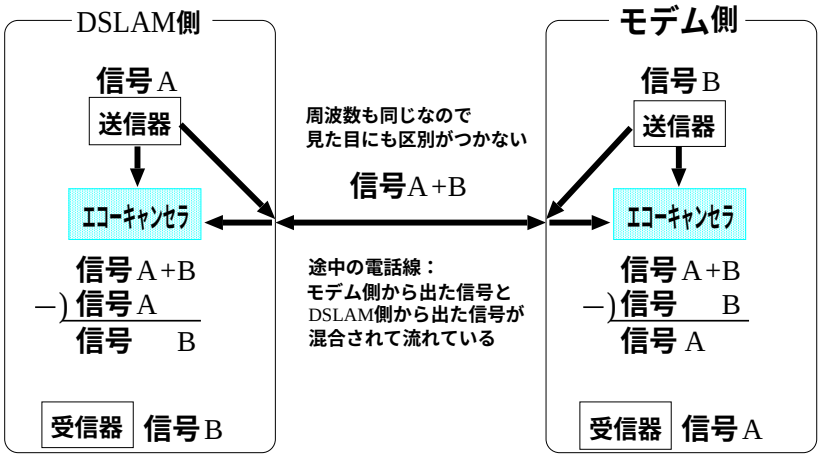

図 B.2　エコーキャンセラの使用例