マルチメディア通信と分散処理　97－5
コンピュータセキュリティ　8－5
（2000．3．21）

著作権保護のための電子透かしシステム

オーディオ電子透かしにおけるマスクの最適配分と次元について

中村大賀　立花隆輝　小林誠士
日本IBM 東京基礎研究所

概要 著作権保護のために電子透かしは重要な役割を担っているが、このような用途には高い信頼性が必要である。オーディオコンテンツへの電子透かしでは検出時に同期操作が必要であるという特徴がある。本論文ではオーディオへの電子透かしの埋め込み・検出手法をモデル化し、エラー率をコントロールするための閾値の設定方法について述べる。同期情報とビット情報へのマスクの最適な配分を求める。さらに正しくないマスクによる検出が統計的に不可能にするのに必要なマスクの次元を求める。

Watermark System for Copyright Protection

Taiga Nakamura　Ryuki Tachibana　Seiji Kobayashi
Tokyo Research Laboratory, IBM Japan, Ltd.

Abstract Watermarking technology plays an important role for copyright protection of audio content. For such application like copyright protection, reliability is one of the most important factor. In this paper, we discuss the method for designing the threshold to fulfill the given error ratio based on the watermark detection model with synchronization, determining the optimum allocation of watermark strength, and for determining the necessary dimension of the masks to statiscally assure false-detection using wrong mask.

1　はじめに

圧縮技術と録音メディアの進歩によりデジタルオーディオの多様な流通形態が可能になった一方、著作権保護への配慮がますます重要になっている。著作権保護のために使われる技術としてはさまざまなものが知られているが、これらを巧妙に連携させることではじめて安全な流通システムが実現する。

音楽コンテンツへの電子透かしでは動画像等の電子透かしとは異なり、「同期」という操作が検出時に必要である。これは動画像にはフレームという区切りがあるのに対し、音楽は一般に連続するストリームであるためである。埋め込みをされた音楽データの一部分からでも検出が可能であるためには、埋め込まれたデータの区切りや先頭を見つける同期が必要になる。

このような検出時の同期を可能にするためには、著作権情報などの内容を運ぶビット情報だけではなく同期情報も音楽データに埋め込まれている必要がある。しかし電子透かしによって音質を劣化させることなく埋め込むことができる情報の量は限られている。

本論文では音楽への電子透かし手法をモデル化し、エラー率を十分低く保つための閾値の設定方法について述べた上で、ビット情報と同期情報を運ぶコンテンツデータの量が限られている状態でビット情報と同期情報をどのような配分にするのが最適であるか、また、誤ったマスクによる検出が統計的に不可能であることを保証するために必要なマスクの次元のサイズについて報告する。

2　技術要求

2.1　電子透かしの役割

コンパクトに圧縮されたデジタルコンテンツはコピーが容易なので、著作権保護の必要性は誰もが認識するところである。著作権保護には暗号・署名・認証・電子透かしなどの技術が一般に使われている。これらの技術が巧妙に連携されてはじめて安全な音楽流通システムは実現する。電子透かしは音楽データ自体を変化させることによって、フォーマットに依存しない方法で著作権情報を音楽に付随させる方法であり、著作権情報の耐性という点では他の著作権保護技術より優れている。

2.2　音楽の電子透かしに対する要請

音楽の電子透かしには次のような要請がある。

- 耐性
  切り取り、D/A 変換、エコー、バンドパスフィル

ター、音声圧縮、イコライザーなどの処理を経た後にも著作権情報が生き残らなくてはならない。

- 3種のエラー
  以下の3種のエラーを考慮しなければならない。

False positive error (以下ではFPEと略記) 埋め込まれてないコンテンツに埋め込みがあると誤検出すること。コピーの許されるコンテンツからコピー禁止情報を誤検出すると利用者の損害になるため、このエラー率は非常に小さく抑える必要がある。

Bit error (以下ではBEと略記) 埋め込みをされているコンテンツから、埋め込まれているのとは違う情報を誤検出すること。もしコピー許可という情報が埋まっているはずのコンテンツからコピー禁止情報を誤検出してしまうとFPE同様に利用者の損害になるので、このエラー率も非常に小さく抑える必要がある。

False negative error (以下ではFNEと略記) 埋め込みをされているコンテンツから、何も情報を検出できないこと。もしコピー禁止情報が埋まっているはずのコンテンツから何も検出ができないと、違法コピーが可能になりコンテンツ所有者の損害となる。FPE率とBE率を小さく保った上で、あらゆる劣化についてFNE率はできる限り小さく抑える必要がある。

3 埋め込み・検出のモデル手法

この章では続く議論の前提として埋め込み・検出のモデル的手法を定義する。

この手法での埋め込みと検出は、コンテンツを変換して得られる一定量の係数列 c の操作によって行う。この変換は離散コサイン変換のようなよく知られた変換手法でもよいが、暗号を使った秘密性を持った手法でもよい。コンテンツのPCMデータをそのまま係数列 c としてもよい。埋め込みでは D_a 個の係数列 c_i に対して同期情報 w_s(常に+1) と B ビットのビット情報 w_b を埋める。係数列 D_a 個のうち D_S 個が同期情報を、1ビット当たり D_B 個がビット情報を運ぶために使う。

$$D_a = D_S + B \cdot D_B \tag{1}$$

1, 0のビット情報は+1と−1として扱う。

$$w_b = +1 \text{ or } -1 \quad (b = 1 \ldots B) \tag{2}$$

3.1 埋め込み

埋め込みは次に説明する手順(図1)によって行う。まずコンテンツおよびそれを変換して得られた係数列 c を用いた感覚モデルを用い、c_i に対する知覚不能な変更量 $\lambda_i(\geq 0)$ を求める。この変更量の大きさだけ、ビット情報、同期情報、マスクに応じて係数列を変更する。

$$c'_i = c_i + \Delta c_i \tag{3}$$

$$= c_i + M_i \cdot w_{bit(i)} \cdot \lambda_i \tag{4}$$

マスク M_i は+1か−1の値をとる疑似ランダム列であり、係数を変更する増減を指定するものである。その役割は、検出時に c_i の影響を打ち消すという働きと、検出時にも同じものが使われなければ検出ができないという意味での鍵としての働きである。

式(4)中で関数 $bit(i)$ は、その係数にビット情報と同期情報のどれを埋めるかを指定する関数である。

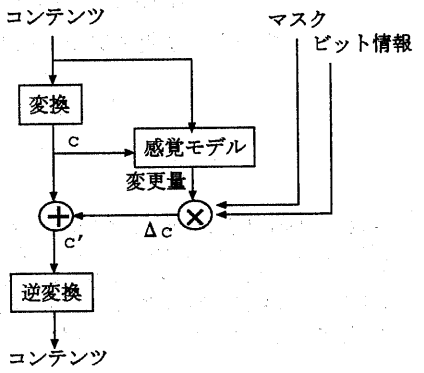

図 1: 埋め込みフローチャート

3.2 検出

検出は次に説明する手順(図2)で行う。検出を始める先頭位置を求め(同期)、求まった同期位置からビット情報を検出する(検出)。何回か検出を行って集まった検出強度を蓄積する(蓄積)。蓄積された検出強度を閾値に対して比較(閾値処理)し、埋め込まれた情報があったか、その情報は何であったかを決定する。

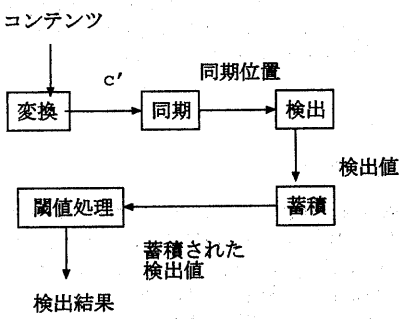

図 2: 検出フローチャート

3.2.1 検出

検出式は次の通り。

$$w'_b = \left(\sum_{i \in loc(b)} M_i c'_i \right) \Big/ \sqrt{\sum_{i \in loc(b)} (c'_i)^2} \tag{5}$$

$loc(b)$ は、b 番目のビットを埋め込んだ係数の集合を求める関数である。その集合の要素数は D_B である。

埋め込みが行われていないコンテンツについては、式(5)は中心極限定理によって標準正規分布に従う。すなわちその確率密度関数 $g_n(x)$ と分布関数 $G_n(x)$ は

$$g_n(x) = \frac{1}{\sqrt{2\pi}} \exp\left[-\frac{x^2}{2}\right] \tag{6}$$

$$G_n(x) = \int_{-\infty}^{x} g_n(t)dt \quad (7)$$

埋め込みが行われているコンテンツでは、式(5)に式(4)を代入すれば

$$w'_b = \frac{\sum_{i\in loc(b)} (M_i c_i + w_b \cdot \lambda_i)}{\sqrt{\sum_{i\in loc(b)} (c'_i)^2}} \quad (8)$$

である。ここでマスクが疑似ランダムなので$\sum M_i c_i$は十分な数の和をとれば0に漸近すると期待できる。よって検出値w'_bは分子の第2項の影響のみが残り、w_bと同符号となる。また、この式中で和を求める要素数はD_Bであるが、D_Bの増加によって分母は$\sqrt{D_B}$のオーダーで増加する一方、分子はD_Bのオーダーで増加する。よって式全体としては$\sqrt{D_B}$のオーダーで増加する。

3.2.2 同期

しかしこの検出式は同期がとれていることを前提としている。同期は、それぞれの検出位置で同期情報の検出を行い、検出結果が最大になる位置を求める。すなわち、ある同期位置$shift$を仮定した同期情報の検出式

$$w'_s(shift) = \frac{\sum_{i\in LS} M_{s,i} \cdot c'_{i+shift}}{\sqrt{\sum_{i\in LS} (c'_{i+shift})^2}} \quad (9)$$

を最大にする位置が同期位置である。LSは同期情報を埋め込んだ係数の集合である。その要素数はD_Sである。

$$w'_{s,\max} = \max_{shift=0}^{N_f-1} (w'_s(shift)) \quad (10)$$

同期位置になりうる位置の数はN_f通りであるとする。埋め込みが行われているコンテンツの正しい同期位置では式(9)は、式(8)同様に埋め込み信号の影響のみが残る。その分布の平均と標準偏差をμ_s、σ_sとする。

埋められていないコンテンツでは式(9)は式(5)同様に標準正規分布に従うので、$w'_{s,\max}$は標準正規分布N_f個から最大値を選んだ分布に従う。その確率密度関数$g_{es}(N_f,x)$と分布関数$G_{es}(N_f,x)$は以下の通りになる。

$$g_{es}(N_f,x) = N_f g_n(x) (G_n(x))^{(N_f-1)} \quad (11)$$
$$G_{es}(N_f,x) = (G_n(x))^{N_f} \quad (12)$$

3.2.3 蓄積

コンテンツには経時的に反復して同じビット情報が埋まっているとする。N_A回検出をした各検出結果w'_bを合計すれば、蓄積した検出結果$\widehat{w}'_b$が求まる。その際、埋めていないコンテンツからの検出強度が標準正規分布に従うように、蓄積回数N_Aを使って正規化する。

$$\widehat{w}'_b = \frac{1}{\sqrt{N_A}} \sum_{i=1}^{N_A} w'_{b,i} \quad (13)$$

埋め込みをしてあるコンテンツからの検出結果はこの蓄積によって$\sqrt{N_A}$のオーダーで強められる。

以下では埋め込んであるコンテンツから検出をした場合の、この$\widehat{w}'_b$の分布が平均μ_b、標準偏差σ_bの正規分布に従うと仮定する。すなわちその確率密度関数$g(x)$と分布関数$G(x)$は次の通りである。

$$g(x) = \frac{1}{\sqrt{2\pi\sigma_b^2}} \exp\left[-\frac{(x-\mu_b)^2}{2\sigma_b^2}\right] \quad (14)$$
$$= \frac{1}{\sigma_b} \cdot g_n\left(\frac{x-\mu_b}{\sigma_b}\right) \quad (15)$$
$$G(x) = \int_{-\infty}^{x} g(t)dt \quad (16)$$
$$= G_n\left(\frac{x-\mu_b}{\sigma_b}\right) \quad (17)$$

3.2.4 閾値処理

あるコンテンツについて埋め込みの有無、埋め込まれたビット情報の判定は次のように行う。まず埋め込みの有無は、埋められたBビットの検出値の絶対値の最小値が閾値T_Bを上回ったかどうかで判定する。

$$\text{埋め込み} = \begin{cases} \text{有り} & (\min(|\widehat{w}'_b|) \geq +T_B \quad b=1\ldots B) \\ \text{無し} & (\text{otherwise}) \end{cases} \quad (18)$$

有りとした場合、ビット情報の判定を次のように行う。

$$\text{ビット情報} = \begin{cases} +1 & (\widehat{w}'_b \geq +T_B) \\ -1 & (\widehat{w}'_b \leq -T_B) \end{cases} \quad (19)$$

4 エラーが起こるケース

2.2章で挙げた3種類のエラーはこのモデルでは次のような場合に起こる。

False positive error (FPE) 埋めていないコンテンツから検出を試みた時に、Bビットすべての検出値が偶然に閾値を上回ってしまった場合。

Bit error (BE) 埋め込み直後のコンテンツ、あるいは埋めた後に劣化をしたコンテンツから検出を試みた時に、すべてのビット検出値が閾値を上回ったが、そのうちの幾つかが埋めた時とは逆の符号で検出された場合。

False negative error (FNE) 埋め込み直後のコンテンツ、あるいは埋めた後に劣化をしたコンテンツから検出を試みた時に、Bビットのうちのどれかのビットが閾値を下回った場合。

5 閾値の設定方法

この章ではビット検出値の閾値T_Bをどのように設定すべきかを説明する。閾値は(1)FPE率を十分低い値に保つ(2)BE率を十分低い値に保つという二つの条件で決まり、より厳しい方を採用するべきである。

5.1 FPE率から決まる閾値

FPE率P_{FPE}はBビットすべてのビット検出値の絶対値が閾値T_Bを上回る確率である。埋めていないコンテンツのビット検出値w'_bは標準正規分布$G_n(x)$に従うので、

$$P_{\text{FPE}} = \{G_n(-T_B) + (1 - G_n(+T_B))\}^B \quad (20)$$
$$= (2G_n(-T_B))^B \quad (21)$$

これをある値$P_{\text{predef,FPE}}$以下であるように設定すると、

$$(2G_n(-T_B))^B \leq P_{\text{predef,FPE}} \quad (22)$$
$$G_n(-T_B) \leq \frac{1}{2}(P_{\text{predef,FPE}})^{\frac{1}{B}} \quad (23)$$

この式と$G_n(x)$の定義式(7)からT_Bは決まる。この式によって求めた、何通りかのBについて$P_{\text{predef,FPE}}$とT_Bの関係を図3に示す。

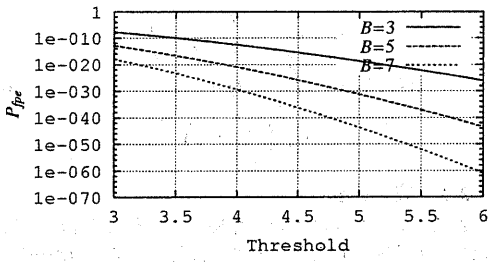

図 3: 閾値 T_B と FPE 率 $P_{\mathrm{predef,FPE}}$ との関係

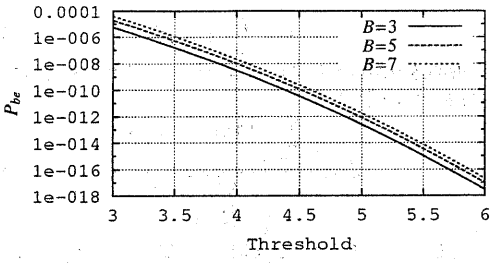

図 4: 閾値 T_B と BE 率 $P_{\mathrm{predef,BE}}$ との関係

5.2 BE 率から決まる閾値

B ビットのうち 1 ビットをパリティチェックに用いてエラー検出をする。この時、検出できないビットエラーは B ビット中に 2 個以上で偶数個のビットエラーが起こった場合である。4 個以上ビットエラーが起きる場合を無視すれば、エラー検出ができないビットエラーが起きる確率 P_{BE} は

$$P_{\mathrm{BE}} = {}_BC_2 \cdot P_e^2 \cdot P_c^{(B-2)} \tag{24}$$

ここで P_e は検出値が誤った符号で閾値を上回る確率、P_c は検出値が正しい符号で閾値を上回る確率である。検出値が分布関数 $G(x)$ の正規分布に従うと仮定すれば、

$$P_e = G(-T_B) \tag{25}$$
$$P_c = 1 - G(+T_B) \tag{26}$$

と書ける。ここで、すべてのビットに+1 を埋めてある (すなわち正しい検出値は正である) と仮定している。これを用いて BE 率は

$$P_{\mathrm{BE}} = {}_BC_2 \cdot G(-T_B)^2 \cdot (1 - G(+T_B))^{(B-2)} \tag{27}$$

これをある値 $P_{\mathrm{predef,BE}}$ 以下に設定するのが目標である。しかし、ビット検出値の分布状態 $G(x)$ はコンテンツの劣化の程度によって異なる。よって以下のような仮定に基づいて安全側から BE 率を抑える。

$$G(-T_B) \leq G_n(-T_B) \tag{28}$$
$$1 - G(+T_B) \leq 1 \tag{29}$$

式 (28) は正の方向に埋めたコンテンツから負の値が検出される確率は、埋め込みをしていないコンテンツから負の値が検出される確率より小さいという仮定である。式 (29) の仮定は自明である。

この二つの仮定に基づけば BE 率の上限は

$$P_{\mathrm{BE}} \leq {}_BC_2 \cdot G_n(-T_B)^2 \tag{30}$$

となり、これを $P_{\mathrm{predef,BE}}$ 以下に設定するには

$${}_BC_2 \cdot G_n(-T_B)^2 \leq P_{\mathrm{predef,BE}} \tag{31}$$
$$G_n(-T_B) \leq \left(\frac{P_{\mathrm{predef,BE}}}{{}_BC_2} \right)^{\frac{1}{2}} \tag{32}$$

この式によって求めた、何通りかの B についての $P_{\mathrm{predef,BE}}$ と T_B の関係を図 4 に示す。

もし FPE 率と BE 率に同じ値を要求する場合、図 3 と図 4 からわかる通り、一般に BE 率から求まる閾値の方が大きな値となるので、実際使う閾値 T_B としてはそちらを採用することになる。

6 マスクの最適配分

この章では、D_a 個の係数列をどれほどの割合で同期情報とビット情報に割り当てるのが最適であるかを求める。

6.1 準備

まず以下の数値を定義する。

マスク配分比 r 利用可能な係数の個数全部に対する、ビット情報の埋め込みに使う係数の個数の比率を表すマスク配分比 r を以下のように定義する。

$$r = \sqrt{D_B / D_a} \tag{33}$$

正しくすべてのビットを検出できる確率を最大化する r を求めるのがこの章の目標である。式 (1) より r の値域は $\left[0, \sqrt{1/B}\right]$ である。

全検出値の平均 μ_a D_a 個の係数列をすべて一つの情報に用いたと仮定した場合の、その検出値の平均。μ_a は、埋め込みをした後にコンテンツが劣化すればするほど小さくなる変数であるので、劣化の程度を表すパラメータでもある。

ビット検出値の平均 μ_b 蓄積されたビット検出値の平均。3.2 節で説明した通り、蓄積された検出値は検出に用いる係数列の数の平方根と、蓄積回数の平方根に比例するので、

$$\mu_b = \sqrt{\frac{D_B}{D_a}} \cdot \sqrt{N_A} \cdot \mu_a \tag{34}$$
$$= r \cdot \sqrt{N_A} \cdot \mu_a \tag{35}$$

同期情報検出値の平均 μ_s 同期情報検出値の平均。μ_b 同様に、

$$\mu_s = \sqrt{\frac{D_S}{D_a}} \cdot \mu_a \tag{36}$$
$$= \sqrt{1 - Br^2} \cdot \mu_a \tag{37}$$

6.2 ビット情報すべてが正しく検出できる確率

ビット情報すべてが正しく検出できる事象 (その確率を P_{OK} とする) は、正しく同期がとれて (その確率を P_{SOK} とする)、同期がとれた状態ですべてのビット検出値が正しく閾値を上回る事象 (その確率を P_{BOK} とする) として表現できる。

$$P_{\mathrm{OK}} = P_{\mathrm{SOK}} \cdot P_{\mathrm{BOK}} \tag{38}$$

6.3 正しく同期がとれる確率

正しい同期位置での同期情報検出値の分布は、平均 μ_s、標準偏差 σ_s の正規分布 (確率密度関数 $g_s(x)$) に従うとする。一方、正しくない同期位置での同期情報検出

値の分布は、埋め込みされていないコンテンツから同期情報の検出を試みた場合の検出値の分布 (式 (11) および式 (12)) に等しいと仮定する。

正しい同期位置が選ばれる確率は、正しい同期位置での検出値が、正しくない同期位置での検出値を上回る確率に等しいので

$$P_{\mathrm{SOK}} = \int_{-\infty}^{\infty} G_{es}(N_f, x) g_s(x) dx \quad (39)$$

$$= \int_{-\infty}^{\infty} \left(\int_{-\infty}^{x} g_n(t) dt \right)^{N_f} g_s(x) dx \quad (40)$$

である。しかし簡単のため以下では次のように単純に近似して扱うことにする。

便宜上、ある評価基準 T_S を次のように導入する。正しい同期位置での同期情報検出値が T_S を上回ったら同期に成功すると近似する。すなわち

$$P_{\mathrm{SOK}} = 1 - G_s(T_S) \quad (41)$$

$$= 1 - G_n\left(\frac{T_S - \mu_s}{\sigma_s}\right) \quad (42)$$

$$P_{\mathrm{SOK}}(r, \mu_a) = 1 - G_n\left(\frac{T_S - \sqrt{1 - Br^2} \cdot \mu_a}{\sigma_s}\right) \quad (43)$$

と近似する。T_S は、正しくない同期位置での検出値が T_S よりも小さい確率が P_s となるように設定する。すなわち

$$P_s = G_{es}(N_f, T_S) \quad (44)$$

$$= (G_n(T_S))^{N_f} \quad (45)$$

$$G_n(T_S) = (P_s)^{\frac{1}{N_f}} \quad (46)$$

何通りかの N_f について P_s と T_S の関係を図 5 に示す。

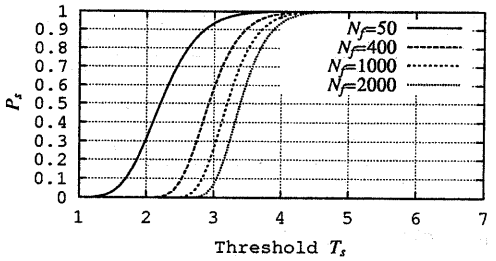

図 5: P_s と T_S の関係

6.4 同期がとれた状態ですべてのビットが正しく検出できる確率

同期がとれた状態でのビット検出値の分布は、平均 μ_b、標準偏差 σ_b の正規分布に従うとする。B ビットがすべて正しく閾値を上回る確率 P_{BOK} は

$$P_{\mathrm{BOK}} = (1 - G(+T_B))^B \quad (47)$$

$$= \left(1 - G_n\left(\frac{T_B - \mu_b}{\sigma_b}\right)\right)^B \quad (48)$$

$$P_{\mathrm{BOK}}(r, \mu_a) = \left(1 - G_n\left(\frac{T_B - r\mu_a\sqrt{N_A}}{\sigma_b}\right)\right)^B \quad (49)$$

配分比 r と劣化状態 μ_a の関数である。ここで、埋め込まれたビットはすべて +1 (すなわち正の側) であるとしている。

6.5 最適配分

式 (43) と式 (49) を式 (38) に代入すれば P_{OK} がマスク配分比 r と劣化状態 μ_a によって表現される。すなわち式 (43)、(49) より、

$$P_{\mathrm{OK}} = G_n\left(\frac{\sqrt{1 - Br^2} \cdot \mu_a - T_S}{\sigma_s}\right) \cdot \left(G_n\left(\frac{r\mu_a\sqrt{N_A} - T_B}{\sigma_b}\right)\right)^B \quad (50)$$

残された問題は標準偏差 σ_s と σ_b である。これはコンテンツが受ける劣化の種類によって異なり、全検出値の標準偏差やマスク配分比の関数として単純に表現することはできない、実験によって定めなくてはならない値である。

標準偏差を 1 として $N_f = 50, B = 5, N_A = 30$ の場合の様々な劣化状態に対して P_{OK} をグラフに表したのが図 6 である。この場合は 0.25 から 0.3 程度の r が最適であるとわかる。図 7 は $N_f = 1000, B = 10$ の場合のグラフである。この場合の最適配分比は 0.2 から 0.25 程度である。ただし $P_s = 0.99$ とした。

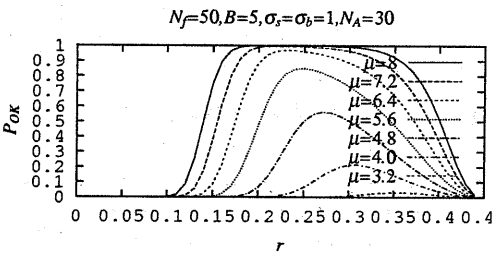

図 6: 様々な劣化状態に対する P_{OK}

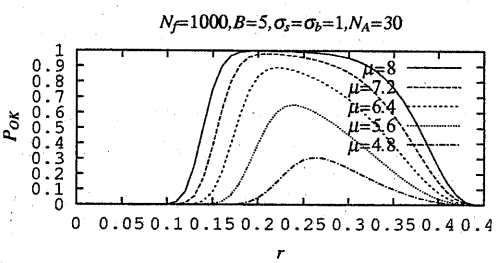

図 7: 様々な劣化状態に対する P_{OK}

7 誤ったマスクでの検出

もしビット検出の際に M_i ではなく別のマスク $\tilde{M}_i$ を用いると、検出式 (8) は次のようになる。

$$w'_b = \frac{\sum_{i \in loc(b)} (\tilde{M}_i c_i + \tilde{M}_i M_i \cdot w_b \cdot \lambda_i)}{\sqrt{\sum_{i \in loc(b)} (c'_i)^2}} \quad (51)$$

$\tilde{M}_i$ と M_i は一部の符号しか一致しないため、正しいマスク M_i を用いて検出した場合よりも検出値は与作なるが、もし $\tilde{M}_i$ が M_i に近ければ同じようにビットが検出できてしまう可能性がある。

正しいマスク以外でもビットが検出できてしまうとするとマスクの鍵としての性格上問題がある。したがって誤ったマスクでビットを検出できる確率が統計的に十分小さいことが必要である。

この章では、異なるマスクからのビット検出率が基準を超える確率を十分小さくするのに必要なマスクの次元について述べる。

7.1 準備

まず以下の数値を定義する。

マスクの一致率 q 2 つのマスク列で値が一致している個数の割合。正しいマスク M_i と任意のマスク $\tilde{M}_i$ の一致率は次式で定義される。

$$q = \frac{D_{(\tilde{M}_i = M_i)}}{D_a} \quad (52)$$

q は $0 \le q \le 1$ の値を取り得る。$q = 1$ のときマスクは完全に一致し、$q = 0$ のときは正負が全く逆のマスクである。ランダムに選んだマスク同士ならばほぼ $q = 1/2$ となる。

正しいマスクによる平均検出強さ μ_M M_i による平均検出強さ。前章における μ_a に相当する。

異なるマスクによる平均検出強さ $\mu_{\tilde{M}}$ M_i とは別のマスク $\tilde{M}_i$ による平均検出強さ。これは、

$$\sum_{i \in loc(b)} (\tilde{M}_i M_i \cdot w_b \cdot \lambda_i) = \sum_{\tilde{M}_i = M_i} (w_b \lambda_i) - \sum_{\tilde{M}_i \neq M_i} (w_b \lambda_i) \quad (53)$$

より、

$$\mu_{\tilde{M}} / \mu_M = \sqrt{q} - \sqrt{1-q} \quad (54)$$

このように平均検出強さの比 $(\mu_{\tilde{M}}/\mu_M)$ が q で表される。

7.2 マスクの一致率 q とビット検出率の関係

一致率が q のマスク $\tilde{M}_i$ による検出率 P_{det} は、式 (50) より次のようになる。

$$P_{\mathrm{det}} = G_n\left(\frac{\sqrt{1-Br^2}(\sqrt{q}-\sqrt{1-q})\mu_M - T_S}{\sigma_s}\right) \cdot \left(G_n\left(\frac{r(\sqrt{q}-\sqrt{1-q})\mu_M\sqrt{N_A} - T_B}{\sigma_b}\right)\right)^B \quad (55)$$

いくつかの B の値について、P_{det} とマスク一致率 q の関係を図 8 に示した。

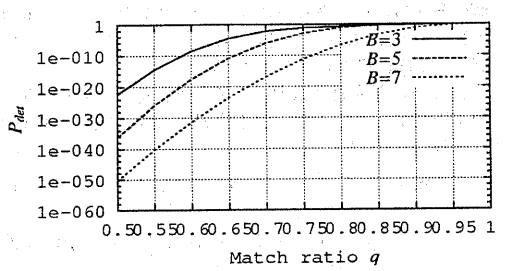

図 8: 検出率 P_{det} とマスク一致率 q の関係

7.3 マスクの次元とマスク一致率の分布の関係

マスク $\tilde{M}_i$ をランダムに選んだとき $\tilde{M}_i$ と M_i のマスクの一致率の分布は二項分布にしたがう。すなわち、マスクの次元が D_a に対して一致率 q がある値 q_{predef} 以上になる確率は、次の通り。

$$P(q > q_{\mathrm{predef}}) = \sum_{i=(D_a \cdot q)}^{D_a} {}_{D_a}C_i \left(\frac{1}{2}\right)^{D_a} \quad (56)$$

マスク一致率 q と検出率 P_{det} は図 8 によって対応づけられる。

したがって、検出率が前もって定めた値 $P_{\mathrm{predef,det}}$ 以上になるようなマスクが全てのマスクの中でどれだけの割合あるかを求めることができる。いくつかの B の値に対して、マスクの次元 D_a と検出率が $P_{\mathrm{predef,det}}$ を超えるマスクが選ばれる確率を図 9 に示した。ただし、$P_{\mathrm{predef,det}} = 10^{-12}$ とする。マスクの次元を十分大きな値にすることによってこの確率を低く保つことが可能である。

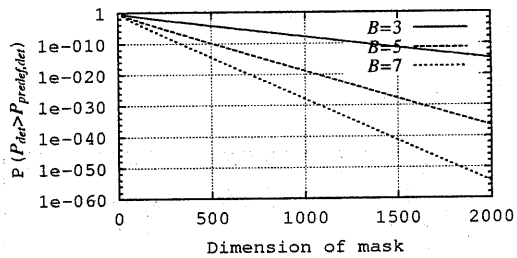

図 9: $P_{\mathrm{det}} > P_{\mathrm{predef,det}}$ となる確率

8 結論

本論文ではオーディオに対する電子透かしのモデルを用いてエラー率を低く保つための閾値を設定し、ビット情報と同期情報を運ぶ音楽データの量が限られている場合にビット情報と同期情報の配分を最適化できることを示した。また、マスクの次元のサイズを十分大きくすることにより誤ったマスクからの検出が統計的に不可能であることを保証できることを示した。