電子演奏の半雑音化と音源符号への電子透かし

岩切宗利[†] 山本紘太郎[†]
関根健一郎[†] 松井甲子雄[†]

インターネットを活用する音楽コンテンツの配信方式は，その市場を拡大できる手段の１つとして注目されている．まず，本研究では，電子楽器の演奏に用いられる SMF（Standard MIDI File）を対象とした電子透かし法を提案する．その方法は，実際の演奏にほとんど影響を与えない音源制御コードや人間の楽器演奏でゆらぎを生じやすい成分へ透かし情報を埋め込むものである．この手法によれば，聴感的に音質を劣化することなく透かしを埋め込むことができる．さらに，半雑音化した演奏音をインターネットを通じて広く試聴させ，コンテンツの購入者には，鍵データで音源コードの雑音成分を除去できる方法を検討し，新しい楽音符号の半雑音化法を提案する．この技術によれば，音源コードから雑音成分を除去した後も透かしを残すことができるので，楽音データをオンライン配信するための基礎技術として有用である．

Half-scrambling and Watermarking Techniques to Computer Music Codes

Munetoshi Iwakiri,[†] Koutarou Yamamoto,[†]
Kenichirou Sekine[†] and Kineo Matsui[†]

In this paper we present a digital watermarking scheme and half-scrambling technique for computer music codes in MIDI (Musical Instrument Digital Interface). Our watermarking method is to change several control codes that give a little effect on the music sound in practice and to embed a watermark bit to the codes corresponding to redundant elements in playing musical instruments. Next, we propose a half-scrambling scheme that enables customer to get sound information on the music through the internet. The partially scrambled sound can be decoded by the paid key, but the watermark embedded above remains in the decoded sound. These techniques may be usable for a new distribution system of music contents.

1. はじめに

コンピュータ技術の急速な発展とインターネット環境の整備にともない，高品質なデジタルコンテンツを容易に利用できる時代になった．特に身近なものとして，電子楽器を用いたデジタル音楽が広く普及している．また，デジタルコンテンツは，インターネットや大容量メディアによって，高速かつ広範に流通し，新たな市場の開拓に大きな役割を果たしている．一方，デジタルデータは，劣化なく容易に複製できるため，著作権侵害の問題が指摘されている．近年，その対策の１つとして，電子透かしが注目されている[1]．これは，コンテンツを流通させる際に，人間が知覚できない形で著作権情報を埋め込む技術であり，不正な横流しの特定や不正行為の心理的抑止に役立てる試みである．

これまでに提案された電子透かしは，画像や映像などの視覚的なコンテンツを対象としたものがほとんどであり[2]，デジタル音声や楽音データを対象とした手法の報告例は少なく，さらに検討が必要である．

音楽コンテンツへの電子透かしやそれに類する試みとして，Boney らによる聴感的マスキングを利用する手法[3]，松井らの量子化雑音に見せかける手法[4]，岩切らの圧縮音声符号に直接埋め込む手法[5)~7)]やスペクトル拡散法[8),9)]，富岡らの音源定位制御法[10)]などがある．これらの技術は，時系列の音響データを対象としたものであり，電子楽器の演奏に用いる MIDI[11)~13)]のような楽音符号[14)]への埋め込みに関する報告例は少ない．

SMF（Standard MIDI File）[11)~13)]を対象とした埋め込み手法として，松本らの情報ハイディング方式が

† 防衛大学校情報工学科
Department of Computer Science, National Defense Academy

ある[15]．これは，同時実行されるイベントのデータ記述順を入れ換えることで，大量の秘密情報を埋め込める手法として興味深い．

本研究では，松本ら[15]とは異なる観点で，SMF を対象とした埋め込み原理を提案し，その特徴について考察した．また，秘密鍵で復号できる楽音データの半雑音化法についても検討した．ここで，半雑音化とは，ある程度の品質で演奏できる状態を保ちつつ，演奏の一部の品質を低下させる処理である．本手法によれば，復号の過程で利用者情報が埋め込まれるため，復号済みコンテンツの著作権も保護できる．

2 章では，SMF の概要を述べる．3 章では，演奏自体を変化させない電子透かし法と，原本性保証の原理について示す．4 章では，音源コードを，聴感的な違和感を与えない程度に制御する電子透かし法を提案する．5 章では，電子楽器の演奏を半雑音化して自由な試聴に供する方法と，その利用契約者には秘密鍵を用いて高品質演奏に復旧する一手法を提案する．

2. SMF の概要

電子楽器の MIDI 1.0 規格[11]のデータ形式である SMF（Standard MIDI File）の概要を示す[11)~13)]．SMF は，ヘッダチャンク（Header Chunk）とトラックチャンク（Track Chunk）によって構成される．ヘッダチャンクは，ファイル全体の情報を最小限の構成（14 バイト）で記述したものであり，トラック数やフォーマット型などの情報が含まれている．一方，トラックチャンク（タイプ MTrk）は，実際のソングデータがストアされるところで，ヘッダチャンクで示されたトラック数だけ存在する．本研究では，各トラックチャンクに含まれるデータセクションのソングデータ（演奏データ）を処理対象とする．

データセクションには，MTrk イベント（MTrk event）とよばれるデータブロックが連続して記述されている．1 つの MTrk イベントは，その直前のイベントからの経過時間を示すデルタタイム（delta-time）と，イベント（MIDI event）から**図 1** のように構成される[11]．

デルタタイム（delta-time）は，最下位のバイトの最上位ビットを “0” とし，それ以外の上位バイトの最上位ビットをフラグ “1” とすることで，**表 1** のように可変長表記している点に特徴がある．表中の記号 “∗” は，数値データとして扱われるビット位置を示している．

一方，イベントコード（MIDI event）は実際の演奏を制御する MIDI メッセージである．たとえば，演奏状態を制御するノートオン（Note On）やノートオフ（Note Off）は，ステータスとノート番号およびベロシティ（音の強さ）で構成される．

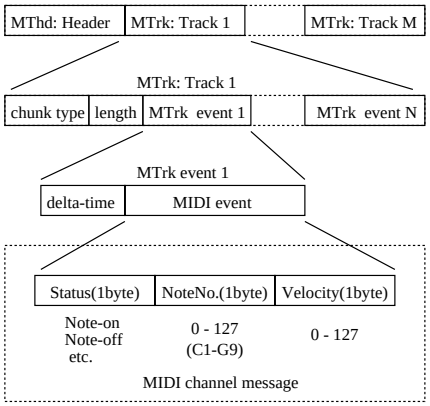


図 1 SMF データセクションの構造
Fig. 1 Structure of SMF data section.

表 1 可変長バイトコード
Table 1 Code system in variable length byte.

Byte	Code expression in binary
1	0*******
2	1******* 0*******
3	1******* 1******* 0*******
4	1******* 1******* 1******* 0*******

3. データ構造利用型の電子透かし

データ構造利用型の電子透かしは，松本らの手法[15]のように，演奏音自体をまったく変化させずに，透かしを埋め込むものである．

3.1 プレフィクス埋め込み法

プレフィクス埋め込み法は，デルタタイムのデータ長に着目して可変長コードに透かしビットを埋め込むものである．MIDI データから選んだあるデルタタイムが，1 バイトであったとき，これを拡張し 2 バイトで表現する．たとえば，78 $(= 4E_{(16)})$ [Tick] は，$804E_{(16)}$ となる．本手法では，この最上位のデータバイト $80_{(16)}$ の有無によって，透かしビット列を埋め込む．すなわち，埋め込むべきビットの値が “1” ならば，デルタタイムの最上位バイトを $80_{(16)}$ とし，埋め込みビット値が “0” ならば，そのままとする．ただし，オリジナルのデルタタイムが最大桁の 4 バイトのときは，それを埋め込みの対象外とした．ここで，オリジナルとは，埋め込みのない状態の MIDI データを意味する．

この単純な埋め込み法を用いて，**表 2** の実験データに**表 3** の署名データを埋め込むと，**表 4** の結果が

表 2 実験用 MIDI データ
Table 2 Experimental MIDI data.

Name (Source file name)	Time [sec]	Events	Size [byte]
Strings (eine_kli.mid)	10	363	1,696
Oboe (water1.mid)	12	750	3,330
Piano (fur_elise_pi.mid)	13	143	745
MusicBox (wewishyou.mid)	14	291	1,241

表 3 署名データ
Table 3 Experimental signature data.

```
23696e636c7564653c737464696f2e683e0d0a0d0a
6d61696e28696e7420617267632c63686172202a61
7267765b5d297b0d0a0d0a09696e74206a2c693b0d
0a09756e7369676e656420636861722207069785b36
353533365d3b0d0a0946494c45202a6670313b0d0a
0d0a096670313d666f70656e28617267765b315d2c
227222293b0d0a0d0a0966726561628706978 2c32
35362c3235362c667031293b0d0a0d0a09666f7228
6a3d303b6a3c36353533363b6a2b2b297b0d0a0909
7069785b6a5d3d7069785b6a5d26307830313b0d0a
09097d0d0a0d0a09666f72286a3d303b6a3c363535
33363b6a2b2b297b0d0a09097072696e7466282225
64222c7069785b6a5d293b0d0a09097d0d0a0d0a09
66636c6f736528667031293b0d0a7d0d0a0d0a0d0a(16)
```

表 4 プレフィクス手法による埋め込み容量
Table 4 Number of bits embedded under prefix method.

	Embedded [bit]	Data size [byte]
Strings	320	1,843 (+147)
Oboe	696	3,649 (+319)
Piano	128	810 (+65)
MusicBox	272	1,370 (+129)

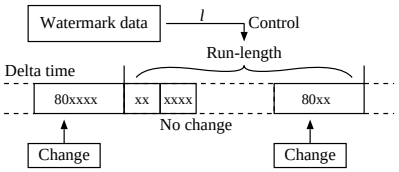


図 2 ランレングス埋め込み法
Fig. 2 Run-length method.

表 5 ランレングスによる埋め込み例（$l = 11$）
Table 5 An example of codes embedded under run-length method ($l = 11$).

No.	Original	Watermarked
0	4E B1 5B 7E	**80** 4E B1 5B 7E
1	0C B1 07 78	0C B1 07 78
2	5A B1 0B 64	5A B1 0B 64
3	14 B1 0A 44	14 B1 0A 44
4	01 B1 5D 1E	01 B1 5D 1E
5	27 B1 5E 01	27 B1 5E 01
6	1E B1 43 3C	1E B1 43 3C
7	8C 72 91 4C 50	8C 72 91 4C 50
8	78 81 4C 00	78 81 4C 00
9	00 91 4B 50	00 91 4B 50
10	78 81 4B 00	78 81 4B 00
11	00 91 4C 52	00 91 4C 52
12	78 81 4C 00	**80** 78 81 4C 00

表 6 ランレングス手法による埋め込み容量
Table 6 Number of bits embedded under run-length method.

	Embedded [bit]	Data size [byte]
Strings	120	1,726 (+30)
Oboe	272	3,398 (+68)
Piano	40	755 (+10)
MusicBox	120	1,271 (+30)

得られた．ここでは，各実験データに埋め込まれたビット数と埋め込み後のデータ量（変化量）を示した．各実験データは，インターネット上に公開されている MIDI データから，異なる特徴の曲を選び，Roland の Ballade 2.1J を用いて約 10 秒ずつ抽出したものである．この結果から，実験データのイベント量に比例して大量の透かしを埋め込めることが分かる．

しかし，すべての可変長データにこの方法で埋め込みを施すと，全体の符号量が大きく増大する問題がある（表 2，表 4 参照）．それを抑制する方法として，次のランレングス埋め込み法を提案する．

3.2 ランレングス埋め込み法

ランレングス法とは，**図 2** のように，埋め込みのある符号間のコード数を透かしで制御する方法である．たとえば，埋め込み符号列から抽出したデータ (l) が 11 ($= \mathtt{b}_{(16)}$) のとき，基点コードから計数して 11 番目のコードを**表 5** のように制御する．すなわち，この手法は，埋め込みのあるコード間のイベント数に透かしを埋め込むものである．一方，透かしビットを抽出するためは，埋め込みのあるコード間のイベント数を調べればよい．

この手法の埋め込み効率（埋め込みビット量/ファイルサイズ増加量）は，**表 6** からプレフィクス埋め込み法（表 4 参照）の約 2 倍になる．ただし，データファイル全体への埋め込み容量は，プレフィクス埋め込み法より減少する．

3.3 符号置換埋め込み法

MIDI1.0 規格[11]の音源コードには，その動作が一般的な音源機器に実装されていないものがある．たとえば，図 1 のノートオフのベロシティ（以下，オフベロシティとよぶ）の動作は，規格として定義されていない．これは，リリースタイムとして利用している一部の音源を除き，使用されていないのが実情である[12]．

表 7 符号置換による埋め込み量（$n = 4$）
Table 7 Number of bits embedded under code replacing method.

Name	Events (note-off)	Embedded [bit]	Data size [byte]
Strings	114	456	1,696 (+0)
Oboe	285	1,112	3,330 (+0)
Piano	53	208	745 (+0)
MusicBox	135	536	1,241 (+0)

ただし，リリースタイムとしての仕様は，MIDI1.0 規格ではないので，本研究では考慮しないものとする．

ここでは，このオフベロシティに着目し，その下位 n ビットを透かし信号列に置き換えることを試みた．この方法を用いれば，楽音データに含まれるノートオフのイベント数に比例して，大量の透かし信号を埋め込むことができると考えられる．また，ファイルサイズおよびイベント数が変化しないことは明らかである．

本手法を用いて，表 2 の実験データに透かしを埋め込んだ結果（$n = 4$）を**表 7** に示す．この結果から，本方式の埋め込みビット数は，各データのイベント数におおむね比例することが分かる．

3.4 デュレーションへの埋め込み法

MIDI シンセサイザ間における高いレベルの互換性を保つ目的で規定され，推奨されている GM（General MIDI system）規格がある[11)~13)]．GM 音源の音色の中には，その特性に応じて，特殊な制御をなされるものがある．この楽器固有の特性を考慮して，音源コードを制御すれば，演奏音を変えることなく透かしを埋め込むことができる．

たとえば，パーカッションの音色は，単純な減衰音である[12),13)]．よって，GM パーカッションマップ（チャネル 10）のドラムサウンド[11)]は，**図 3** のようにノートオフを無視する実装をしている音源が多い[13)]．ここでは，パーカッション音のノートオフのタイミングを制御することで，そのデュレーション（**図 4** 参照）に透かしを埋め込むことを考える．

デュレーション（Duration）とは，ある演奏音のノートオンからノートオフまでの間にあるイベントのデルタタイムの合計値である．埋め込みは，ノートオフのデルタタイムの最下位ビットを透かしビットで置き換える方式を用いた．また，埋め込みにより変化した時間のずれについては，その次のイベントのデルタタイムで相殺できる．

本研究では，簡単のために最下位ビットのみを埋め込み制御したが，実際はさらに上位のビットを制御しても，演奏には影響しないと考える．また，SMF 規格に定義されているデルタタイムの分解能を，細かく

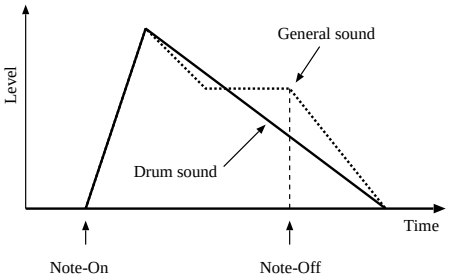


図 3 ドラム音の減衰特性
Fig. 3 Attenuation characteristic of drum sound.

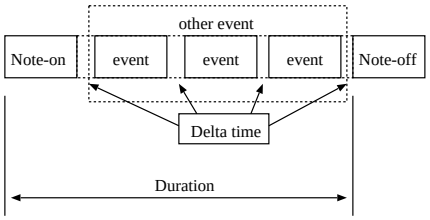


図 4 デュレーション
Fig. 4 Duration.

設定すれば，埋め込み容量を増大できる．分解能の前処理は，デルタタイムを操作するタイプの埋め込み手法全般に有効である．

ただし，このような特殊な音源の仕様を利用する埋め込み技術は，MIDI 機器によって利用できない場合があることに注意する．

3.5 演奏実験と動作確認

Roland 社製の SC-55mkII および YAMAHA 社製の MU2000 をコンピュータにシリアル接続して，透かしを埋め込み済みの MIDI データを用いて演奏実験を行った．その結果，各音源の動作に問題を生じないことが確認できた．また，**図 5** のように，埋め込みのある実験データによる再生波形とオリジナルの再生波形と比較し，それらが一致することを確認した．

3.6 原本性保証への応用

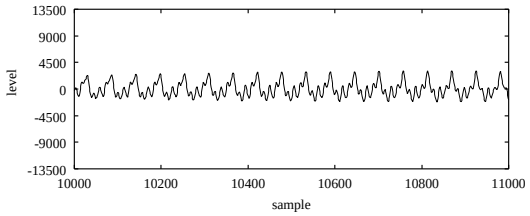
これまでに提案した電子透かし技術を原本性保証の技術として利用することを考える．MIDI データの原本性とは，配布した MIDI データが改変されていない状態であることを意味する．

前節までに検討した方法は，SMF のデータ構造の自由度を利用して電子透かしを埋め込む技術である．一方，一般的な楽音編集ソフトウェアは，データファイルから MIDI データをメモリへ読み込む際に，ファイル（SMF）のデータ構造を破棄し，独自の処理しやすいデータ形式へ変換する．たとえば，可変長コードを利用した透かし信号 $80_{(16)}$ は，読み込む際に値

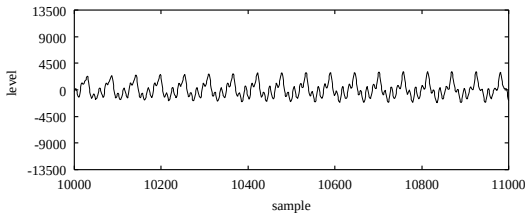
0 [Tick] として無視されるため，完全に消失する特性がある．また，符号置換による透かし信号である音源コードは，ソフトウェア規定のコードへ置き換えられることも多い．したがって，本章で述べた手法で埋め込まれた透かし信号は，一般的な編集ソフトウェアでメモリへ読み込むだけで消失すると考えられる．

そこで，本手法を用いて，原本性を保証する未編集符号を音楽コンテンツへ埋め込むことを提案する．すなわち，MIDI データに何らかの操作が加えられることで，電子透かしが消失する仕組みにする．これは，MIDI のデータファイル（SMF）の原本性を保証するための一手法として有用であると考える．

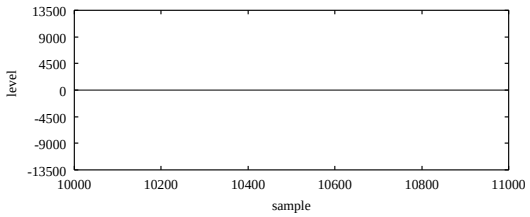
実際に，複数の楽音編集ソフトウェアを用い，実験



(a) Decoded waveform of music box sound without watermark



(b) Decoded waveform of music box sound with watermark



(c) Difference waveform

図 5 音声波形の比較
Fig. 5 Comparison of sound waveform.

データをメモリへ読み込み，“まったく編集操作しない状態” でデータディスクへ記録した．この簡単な操作を受けたデータファイルに，透かし信号が残存しているかどうかを調べた結果，**表 8** が得られた．実験の結果から，デュレーションへの埋め込み手法を除く手法で，埋め込まれた透かし信号は，完全に消失することが分かった．

また，デュレーションを用いた電子透かし技術で埋め込まれた透かし信号は，一部のソフトウェアの処理で消失するものの，ほとんどの場合で残存できた．これは，デュレーションを利用した埋め込み信号が，演奏曲の流れ（コンテンツの主要素）に強く依存しているためであると考える．このように埋め込み処理を工夫することで，透かしの残存性を高めることもできる．

ここで考察したように，データ構造利用型の電子透かしは，画像や電子文書などの原本性保証技術にも応用できる可能性がある．

4. 演奏情報制御型の電子透かし

人間の聴覚の曖昧さに冗長性を見いだし，透かし情報を冗長部分に埋め込む方法がある．このタイプの電子透かしは，画像や音響データの分野で数多く検討されている．しかし，MIDI のような楽音符号に対して提案された報告は，いまだ見当たらない．

一方，人間が楽器を演奏する際に，発音タイミングや音量は，つねに一定ではないと考えられる．むしろ，人間の演奏時に発生するわずかな変動は，微妙な効果として，より芸術的な演奏を実現し，楽曲に表情を付ける要素となる[14]．

MIDI のようにコンピュータで音源を直接制御すると，つねに一定かつ正確な演奏を再現できる．この特徴は，より精緻な演奏を実現できる一方，聴者に機械的な印象を与えやすい．この対策として，演奏家のくせをパラメータ化し，コンピュータによる演奏を，より自然にする試みもなされている[14]．

4.1 ベロシティ埋め込み法

ノートオンのベロシティ（以下，オンベロシティと

表 8 編集操作による電子透かしの検出
Table 8 Lossy check of watermark for protecting original contents.

Software	Delta-Time	Off-Velocity	Duration
Cake Walk Pro 5.0J *1	Vanish	Vanish	Vanish
Singer Song Writer *2	Vanish	Vanish	Exist
Cherry 1.4.3 [16]	Vanish	Vanish	Exist
Ballade 2.1J *1	Vanish	Vanish	Exist

*1: Roland, *2: Internet

表 9 埋め込みビット位置
Table 9 Position of bits to be embedded in velocity.

$V_{(2)}$	$\lfloor \log_2 V \rfloor$	n	$V'_{(2)}(p=4)$
01******	6	p	01**wwww
001*****	5	$p-1$	001**www
0001****	4	$p-2$	0001**ww
00001***	3	$p-3$	00001**w
000001**	2	$p-4$	000001**
0000001*	1	$p-5$	0000001*
00000001	0	$p-6$	00000001

よぶ）は，図 1 に示すように演奏音の強弱を制御する 7 ビットのパラメータである[11]．これは，人間が演奏する場合，その曲が持つイメージを表現する要素の 1 つに相当する．すなわち，楽曲中の音の強さは，つねに一定でフラットな状態であるより，むしろ微妙な変動や雑音が存在した方が，演奏の質感を高められると考えられる[14]．そこで，音の強弱をコントロールするオンベロシティの下位ビットを，透かし信号で置換する方法を用いて音質の変化を調べた．

ここで，MIDI データから抽出したオンベロシティ値を V とし，埋め込み強度を制御するパラメータを p ($p \leq 6$) とする．p は，V に埋め込む透かしのビット数 n の最大値を制御するパラメータである．埋め込み処理は，単純に V の下位 n ビットを透かしビットに置き換える手法を用いた．n は V の大きさに適応して，**表 9** のように定める正値である．この表では，オリジナル V の不特定なビット値を “*” で示している．また，$p=4$ のときの埋め込み可能なビットは，表 9 の “w” である．ここで，$n \leq 0$ のときは，埋め込み対象外としていることに注意する．

4.2 音質への影響

音質の評価法として，20 代の被験者 13 名の主観的絶対値によるオピニオン評価[17]を用いた．これは，提示した演奏音の品質を 5 段階評価させ，得られた評価値から平均オピニオン値（MOS: Mean Opinion Score）を求めるものである．各オピニオン値の基準は，オリジナルと判別できない状態を 5 とし，差異が著しい状態を 1 とした．

音質を評価する際は，モニタヘッドホンを個別に装着させ，実験データの演奏とオリジナルの演奏を自由な回数だけ聴き比べさせた．また，被験者の先入観による影響を避けるため，埋め込みのあるものとオリジナルデータを区別できない状態で準備した．埋め込みによって，聴感的な音質の劣化が感じられたならば，MOS に大差が生じるはずである．

実験の結果，**表 10** の評価値が得られた．表中の $p=0$ は，オリジナルを評価させた場合のものである．これらの結果から，実験データによって多少のばらつきがあるものの，$p=4$ 程度までならば，オリジナルと同等の品質を維持し，違和感を与えないことが分かった．

表 10 p と音質 MOS の関係（ベロシティ）
Table 10 Mean opinion score with parameter p.

p	0	1	2	3	4	5	6
Strings	4.69	4.38	4.69	4.08	3.38	3.23	2.31
Oboe	4.31	4.31	4.46	4.00	4.00	3.08	2.00
Piano	4.08	4.08	4.38	4.62	4.31	2.77	1.31
MusicBox	4.00	4.46	4.54	4.54	4.31	4.31	2.69

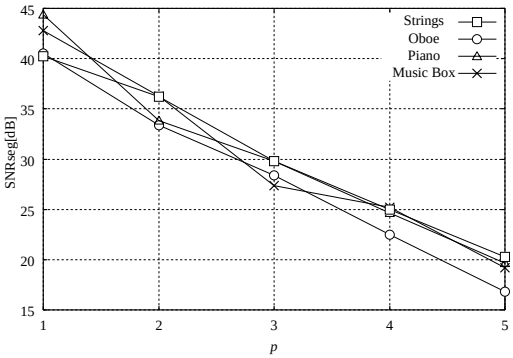


図 6 p と $\mathrm{SNR}_{\mathrm{seg}}$ の関係
Fig. 6 Segmental SNR with p.

また，p が 2〜3 のときに，オリジナルより高い評価値が多く出現している点も興味深い．これは，演奏音の感覚的な品質が，埋め込みによりオリジナルと判別できない範囲で，微妙に向上した可能性を示している．被験者の中には，埋め込み強度の高い演奏 $p=5$, 6 の方が，演奏に抑揚があって好ましいとコメントする者もいた．

また，演奏音を客観的に評価するため，各実験データから再生される音声波形を 44.1 kHz で標本化し，16 ビット量子化による 1 チャネルのデジタル音響データとした．波形の比較には，音質の客観的評価法として知られるセグメンタル SNR（以下，$\mathrm{SNR}_{\mathrm{seg}}$）を用いた[17]．

透かし情報を埋め込み済みの実験データとオリジナルデータから得られる波形を比較した結果を**図 6** に示す．この結果から，埋め込み強度 p が大きくなるに従い $\mathrm{SNR}_{\mathrm{seg}}$ も低下することが分かる．本手法は，音そのものの成分を操作せずに，その強弱を制御するものであるため，表 10 に示したとおり，音質はそれほど低下していないことに注意する．

5. 半雑音化と電子透かし

MIDI ファイルそのものを暗号化し，そのままでは演奏できない状態で配布することは容易である．しかし，ある程度音楽として楽しむことができる MIDI データを，試聴用として広く提供することができれば，新たな顧客を得る市場開拓に役立つと考えられる．実際に，映像や画像配信の業界では，その試みで高い効果をあげている．

デジタル音響データや楽音データを対象とした試聴システムとして，演奏の一部や演奏パート数を制限した状態で配信することが考えられる．このような手法では，試聴用データをあらかじめ準備し，その試聴結果から購入者が決まる．その際に利用権を購入した者にあらためて完全なデータを再配信しなければならない．しかし，この手順は頻雑なので，試聴版から秘密鍵で原本を復元可能であるならば，音楽コンテンツの配信システムは簡潔となり，インターネットコマースの基盤技術として有用であろう．

現在のところ，このような目的から音楽コンテンツを半雑音化し，配信する手法の報告例[18]は少ない．本研究では，半雑音化による試聴システムを実現する電子透かしについて検討した．

5.1 短期イベント撹拌法

本手法では，まず図 1 に示す楽音データの中から m 個の発音イベントの音源コード（音の高さと強さの情報）をランダムに選ぶ．これらを演奏順に時間軸上に並べる．一方，重複しないように 2 つの乱数 r_1, r_2 $(1 \le r_i \le m)$ を生成する．次に**図 7** に示すように，これらの m 個の音源コードのうち，r_1 番目と r_2 番目の音源コードを入れ換える．これを n 回繰り返す．その結果，電子楽器で演奏できる状態のまま，スクランブルをかけたことになる（**表 11** 参照）．

このとき，一定区間内の m 個のコードに対して並べ換えるコードの割合を

$$\gamma = \frac{2n}{m} \qquad (1)$$

で表し，ランダム化率と定義する．この γ を調節することで，半雑音化のレベルを制御することができる．一方，半雑音化された楽音データを元の状態へ復号するには，雑音化の際に並べ換えた音源コードを元の状態へ戻せばよい．

この方法によれば，音源コードの大半が変更されていない状態であり，一部分のみ半雑音化のもとで演奏されるため，試聴に際し原曲の雰囲気を大略理解することができる．ただし，演奏のリズムが損なわれると，原曲の雰囲気を大きく損なうため，ここでは，音の高さと強さのみを操作していることに注意されたい．

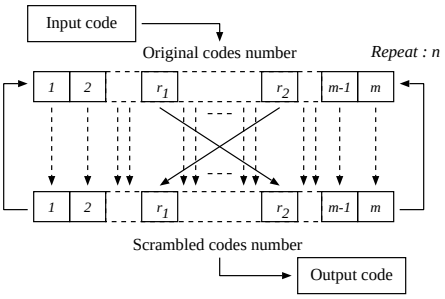


図 7 短期イベント撹拌法
Fig. 7 Short-terms event scrambler.

表 11 半雑音化コードの例（$m = 15$, $n = 2$）
Table 11 An example of codes scrambled in short-terms ($m = 15$, $n = 2$).

Time	No.	Original	Scrambled
0	1	91 **47 50**	91 **4C 50**
	2	91 4B 50	91 4B 50
	3	91 4C 52	91 4C 52
	4	91 4B 54	91 4B 54
	5	91 4C 57	91 4C 57
	6	91 47 5A	91 47 5A
	7	91 4A 56	91 4A 56
	8	91 **44 50**	91 **48 53**
	9	91 45 50	91 45 50
1	10	91 3C 50	91 3C 50
	11	91 40 50	91 40 50
	12	91 45 50	91 45 50
	13	91 **4C 50**	91 **47 50**
2	14	91 40 50	91 40 50
	15	91 **48 53**	91 **44 50**

表 12 ランダム化率 γ と MOS の関係
Table 12 Relationship between γ and MOS.

γ	0.00	0.05	0.10	0.15	0.20	0.25
Strings	4.67	4.67	4.67	4.44	4.78	2.11
Oboe	4.67	3.67	3.67	3.33	3.00	3.56
Piano	4.89	4.78	2.78	2.44	2.78	1.44
MusicBox	4.67	3.89	3.33	3.22	2.33	2.11

半雑音化手法による実験では，一定の符号区間（コード数固定）で，ランダム化率を変化させ，オリジナル曲の雰囲気を聴者が感じられるか否かを判定させた．**表 12** に，$m = 40$ のもとで各ランダム化率 γ ごとに評価した結果を示す．この結果は，MOS と同様にオリジナルの演奏をあらかじめ聴取させ，γ の異なる再生音を不特定に 9 名の被験者に提示して評価させたものである．特に $\gamma = 0$ は，オリジナルを演奏したときの評価値を示す．これらの結果から，雑音化制御のコード区間の長さが $m = 40$ の場合，適切なランダ

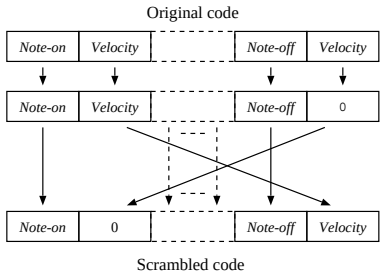


図 8 音源コード無効化の処理
Fig. 8 Sound code invaridating technique.

ム化率 γ は 0.1〜0.2 程度であることが分かる．

5.2 音源コード無効化法

ノート情報の中でも，ノートオフのベロシティ[12),13)]は，演奏に影響しない点に着目し，半雑音化法する手法を検討した．まず，**図 8** のように，ノートオンとノートオフの組を選び，オフベロシティのみを 0 として，それぞれのベロシティを入れ換える．この方法により任意のコードをランダムに消音化できる．さらに，オフベロシティの値をあらかじめ乱数化しておけば，消音ではなく音の強さが不自然に変動することになる．これは，半雑音化の一手法としてより効果的に利用できると考えられる．

また，本手法で半雑音化されたデータを一般的な楽音編集ソフトウェアで読み込むと，3 章で述べた原理によって，オリジナルのデータが消失するため復号できなくなる．これは，不正なデータ編集を困難にする効果がある．ただし，単にベロシティを入れ換えるだけでは，それを元へ戻すだけでオリジナルへ復号されるおそれがある．その対策として，あらかじめオリジナルのオンベロシティ値を暗号化しておくことが望ましい．

5.3 埋め込み機能付き復号鍵利用法

音源コードのオンベロシティをランダム化すると，演奏曲を変えることなく，音の強さが不均一な状態になる．そこで，オンベロシティに着目して半雑音化し，それを復号する過程で透かしを埋め込む方法を次に提案する．

まず，MIDI コードの中からオンベロシティ V を選ぶ．これに 7 ビットの乱数 R を排他的論理和する．すなわち，半雑音化された状態のオンベロシティ V'' は，

$$V'' \leftarrow V \oplus R \tag{2}$$

となる．このオンベロシティがランダム化された MIDI データを試聴用とする．次に，4 章の電子透かし法で，オリジナルのオンベロシティ V へ利用者の個人情報 W を埋め込み，V' を生成する．この V' と V'' を用いて，透かしの埋め込み機能付き復元鍵 K を生成する．

$$K \leftarrow V'' \oplus V' \tag{3}$$

この K を用いれば，半雑音化した状態から

$$V'' \oplus K = V'' \oplus V'' \oplus V' \quad \rightarrow \quad V' \tag{4}$$

のように高品質な状態 V' を合成できる．この V' は 4 章の考察から，利用者が埋め込みの存在を判別できない高品質な状態である．また，V' は，利用者情報などの電子透かしが埋め込まれている状態であることに注意する．この方法は，復号の過程で利用者自身の手によって透かしを埋め込む点に特徴がある．すなわち，この利用者情報を示す透かしの存在が，その音楽コンテンツの正規ユーザであることの証明になる．

5.4 電子透かしと半雑音化

コンテンツの半雑音化帯域とそこに埋め込まれた透かし帯域は互いに独立している．これは，半雑音化したデータを復号したあとも埋め込まれた透かし成分が残存できることを意味する．すなわち，著作権情報が埋め込まれた MIDI データをそのまま半雑音化できるのである．

これらの技術を適切に組み合わせれば，MIDI データの試聴配信システムを構築できる．利用者は，試聴配信システムを用いることで，どのような商品であるかをコンテンツ購入前に知ることができる．一方，データ配信者は，利用者に商品価値の高いコンテンツの試聴データを提供し，その購買意欲を高揚できるであろう．半雑音化は，演奏できる状態のままコンテンツを暗号化する点で，従来の暗号とは異なる特徴を持つ．したがって，この技術は，将来のオンライン配信の基礎技術として有用と考えられる．

6. おわりに

本研究では，楽音符号のデータ形式として，広く知られている MIDI ファイルに透かしを埋め込む技術をいくつか提案した．これら手法を用いると，聴感的な音質をほとんど劣化することなく，著作権情報などを埋め込むことができる．また，MIDI データをランダムに制御することで，演奏音を半雑音化する手法を新たに提案した．これらの手法を適切に組み合わせて使用すれば，MIDI データの試聴配信システムとして利用できると考える．

今後の課題として，高度なセキュリティ技術の導入による透かしの改竄防止，各埋め込みパラメータおよび半雑音化パラメータの適切な設定法の開発があげら

れる．さらに適切な客観的音質評価法が確立できれば，埋め込みによって聴感的な品質を向上しつつ，透かしを埋め込める電子透かしの開発も可能であろう．

参 考 文 献

1) 松井甲子雄：電子透かしの基礎—マルチメディアのニュープロテクト技術，第 7 章，森北出版 (1998).
2) 電子透かし技術に関する調査報告書，日本電子工業振興協会 (1999).
3) Boney, L., Tewfik, A.H. and Hamdy, K.N.: Digital watermarks for audio signals, *Proc. International Conference on Multimedia Computing and Systems*, pp.473–480 (1996).
4) 松井甲子雄，中村康弘，ナタウットサムパイブーン：音声通信への文字情報の埋め込み，第 18 回情報理論とその応用シンポジウム，pp.389–392 (1995).
5) 岩切宗利，松井甲子雄：適応差分 PCM 符号化における音声符号へのテキスト情報の埋込み，情報処理学会論文誌，Vol.38, No.10, pp.2053–2061 (1997).
6) 松井甲子雄，岩切宗利：低遅延符号励振線形予測符号化による音声符号への電子透かし，画像電子学会誌，Vol.27, No.5, pp.475–482 (1998).
7) 岩切宗利，松井甲子雄：共役構造代数符号励振線形予測による音声符号へのテキスト情報の埋込み，情報処理学会論文誌，Vol.39, No.9, pp.2623–2630 (1998).
8) 岩切宗利，松井甲子雄：スペクトル拡散と変形離散コサイン変換による高品質デジタル音声のための電子透かし法，情報処理学会論文誌，Vol.39, No.9, pp.2631–2637 (1998).
9) 岩切宗利，松井甲子雄：周波数ホッピングによるデジタル音楽への電子透かし法の提案，信学技報 ISEC2000-28，Vol.100, No.213, pp.33–40 (2000).
10) 富岡淳樹，中村高雄，小川 宏，高嶋洋一：マルチチャネルディジタルオーディオに対する電子透かし，1998 年電子情報通信学会情報・システムソサイエティ大会，D-14-4, p.323 (1998).
11) 音楽電子事業協会：MIDI1.0 規格書，リットーミュージック (1998).
12) 中島安貴彦：MIDI バイブル I，リットーミュージック (1997).
13) 中島安貴彦：MIDI バイブル II，リットーミュージック (1998).
14) 長嶋洋一，橋本周司，平賀 譲，平田圭二：bit 別冊コンピュータと音楽の世界，共立出版 (1998).
15) 松本 勉，井上大介，北林創太：演奏データファイル SMF への情報ハイディング方式，2000 年暗号と情報セキュリティシンポジウム，SCIS2000-C03 (2000).
16) ベクターデザイン編：Pack for Win 1999 年後期版，メディアワークス (1999).
17) 小澤一範：ディジタル移動通信のための高能率音声符号化技術，トリケップス (1992).
18) 岩切宗利，松井甲子雄：オンライン配信のための音楽への電子透かし法，2000 年暗号と情報セキュリティシンポジウム，SCIS2000-C01 (2000).

(平成 13 年 5 月 31 日受付)
(平成 13 年 12 月 18 日採録)

岩切 宗利（正会員）

昭和 45 年生．平成 5 年防衛大学校情報工学科卒業．平成 10 年防衛大学校理工学研究科情報数理専攻修了．平成 11 年防衛大学校情報工学科助手．マルチメディアと情報セキュリティに関する研究に従事．電子情報通信学会，日本音響学会，画像電子学会，映像情報メデイア学会会員．

山本紘太郎

昭和 53 年生．平成 13 年防衛大学校情報工学科卒業．マルチメディアと情報セキュリティに関する分野に興味を持つ．

関根健一郎

昭和 53 年生．平成 13 年防衛大学校情報工学科卒業．マルチメディアと情報セキュリティに関する分野に興味を持つ．

松井甲子雄（正会員）

昭和 14 年生．昭和 36 年防衛大学校電気工学科卒業．昭和 40 年九州大学大学院工学研究科電子専攻修了．昭和 56 年防衛大学校電気工学科教授．平成元年同大情報工学科教授．この間暗号学，情報セキュリティ，電子透かし，音声・画像データの符号化に関する研究に従事．工学博士．電子情報通信学会，画像電子学会，映像情報メデイア学会会員．著書「電子透かしの基礎」（森北出版）で第 15 回電気通信普及財団賞受賞．