編集ソフトウェアの特徴を利用した攻撃への耐性を有するSMFステガノグラフィ

遠山 毅[†] 鈴木雅貴[††]
四方順司[†] 松本勉[†]

ステガノグラフィは本当に伝えたい情報を見せかけの媒体に隠すことで，通信をしている事実そのものを秘匿する技術であり，画像や音声，テキストなど，様々な媒体を用いる方式が研究されている．その中で，井上・松本によって，演奏データファイルである SMF（Standard MIDI File）を媒体としたステガノグラフィ方式が提案されており，この方式のステゴ解析への耐性に関して，インターネット上で配布された SMF の特徴を考慮した解析による評価が行われてきた．本稿では，SMF に記述された同時ノートの並びが SMF の編集ソフトウェアの影響を受けることに着目して，編集ソフトウェアが同時ノートに残す特徴を考慮した埋込み方式を提案する．また，提案方式の拡張として，ある SMF に対して適用可能な提案方式であり，かつ適用した際，ステゴ SMF の検出攻撃に対する耐性が同じになる方式の中から最も埋込み可能情報量の多い方式を採用する方式を提案する．埋込み方式の評価としてインターネット上の SMF 約 18,000 曲に対して埋込み可能情報量を計測した結果，提案方式を用いて埋め込んだステゴ SMF は以下のような特徴を持つことが分かる．まず，安全性の面では，編集ソフトウェアの特徴を考慮した埋込み検出攻撃に対する耐性を持つため，秘匿性が向上したと考えられる．しかしながら，効率性の面では，埋込み可能情報量と埋込み可能 SMF 数がともに減少することが見受けられる．

Methods of Standard MIDI File Steganography Resistant against Attacks Using Characteristics of Editing Software

Tsuyoshi Toyama,[†] Masataka Suzuki,[††] Junji Shikata[†] and Tsutomu Matsumoto[†]

The purpose of steganography is to make communication innocent by hiding genuine information in innocuous cover-object. Several steganographic schemes that use image, sound, text, etc. as cover object have been developed. In particular, Inoue, et al. proposed the SMF steganographic scheme in which SMFs (standard MIDI files) are used as cover-object, and they evaluated this scheme in terms of the characteristics of SMFs downloaded from the websites. In this paper, we focus on the fact that the SMF editors characterize SMFs, and propose embedding methods by taking into account the characteristics of SMF editors. Based on these methods, we also propose embedding methods that can achieve highest embedding rates within applicable methods for a SMF. Furthermore, we show that our proposed methods are more resistant to the steganalysis than previous methods, while both of amount of embedding information and the numbers of embeddable SMFs tend to be more decreased in our methods.

1. はじめに

ステガノグラフィとは，本当に伝えたい情報（Embedded Data）を見せかけの情報（Cover Data）に埋め込み，この情報とほとんど性質の変わらない情報（Stego Data）を生成し，これを送受信することによって，通信当事者以外のエンティティに対して，まさに伝えたい情報の通信の存在自体を守秘することを目的とした技術である．

ステガノグラフィは，通信内容の守秘を目的とした暗号通信と比べ，通信の存在の守秘を目的としている点で異なるため，Cover Data として利用する情報は，

† 横浜国立大学大学院環境情報学府/研究院
Graduate School of Environment and Information Sciences, Yokohama National University
†† 日本銀行
Bank of Japan

本稿は，研究発表論文 7)，8) の内容に，SMF のファイルフォーマット 1 に関する考察を加えたものである．

世の中で広く普及しているメディア・データフォーマットや，広く使われているプロトコルなどが望ましい．

我々は，インターネット上で楽曲を配信するための一手段として広く利用されている SMF（Standard MIDI File）を Cover Data として利用する方式に注目する．

SMF を利用したステガノグラフィ方式は，井上・松本によって最初に提案されている[5]．この方式によって埋め込まれた SMF が持つ特徴は，インターネット上で配布されている多くの SMF が持つ特徴と異なる特徴を持つため，SMF に埋込みが行われているか否かが検出できる．そこで，埋込みを行っても，インターネット上で配布されている SMF と見分けがつかないように改良した埋込み方式が提案されている[6]．

そのほかに SMF を利用した情報ハイディングの方式として，松井・岩切らにより，可変長表記を利用した方式や，表情付けを考慮したうえでノートオフの位置やベロシティに埋め込む方式などが提案されている[9),10)]．これらの埋込み方式は，井上・松本方式と埋込み箇所が独立しているため，1 つの SMF に対し，複数の方式を併用することが可能である．ただし，各方式による埋込み情報が消失しないよう，注意する必要がある．たとえば，井上・松本方式を適用して埋め込んだ SMF に対し，ノートオフの位置を変更して埋め込む方式を適用した場合，そのノートオフが構成していた同時ノートが消失する可能性がある．この場合，ノートオフの位置を変更して埋め込んだ後，井上・松本方式によって埋め込むことで対応できる．

本稿では，文献 5)，6) で提案された方式の発展として，シーケンサで作成された SMF と区別がつかないように埋め込む方式を提案する．文献 6) では，インターネット上の SMF を観察することで，多くの SMF が持つ特徴を解析し，その特徴を持たせて埋め込むことで秘匿性を向上させた方式を提案していた．しかし，これらの特徴は SMF 編集ソフトウェア（以下シーケンサ）に由来することが予想されるため，インターネット上の多くの SMF が持つ特徴を模倣するだけでは，個々のシーケンサが SMF に残す詳細な特徴を知る攻撃者には，埋込みがなされている SMF かそうでないかが判別できると考えられる．つまり，個々のシーケンサが SMF に残す特徴を直接解析し，その特徴を持たせつつ埋め込むことで，より秘匿性の高い方式が提案できるといえる．そこで本稿では，シーケンサの特徴を考慮した埋込み手法を提案し，代表的なシーケンサを例に具体的な方式を示す．また，本稿で取り扱う代表的なシーケンサ以外にも数多くのシーケンサが存在し，今後も数多く開発されていくであろうと予想されるが，それらのシーケンサについても，SMF に残す特徴を解析することで，本稿で提案する手法が適用できるといえる．

さらに，この埋込み方式を拡張した M-∗ 方式を提案する．複数のシーケンサに対しそれぞれ埋込み方式が考えられる．そこで，ある SMF に埋込みを行う際，その SMF に適用でき，かつ，耐性が同じ埋込み方式が複数存在する場合は，最も埋込み可能情報量の高い方式を採用するように拡張する．

提案方式の評価として，各方式の性能測定実験を行う．具体的には，各方式の埋込み率と適用できる SMF の割合を測定する．

以降，次章で SMF ステガノグラフィの概要と，解析者による埋込み検出に耐性を持つ埋込み手法について議論する．3 章では編集ソフトウェアの特徴を考慮した埋込み手法を提案し，提案手法を基にした具体的な埋込み方式とそれを用いた M-∗ 方式について提案する．そして，4 章では提案方式について考察を行い，5 章でまとめる．

2. SMF ステガノグラフィ

本章では SMF ステガノグラフィについての説明を行う．まず，2.1 節で，埋込みの媒体に使用している SMF について述べ，2.2 節で，SMF ステガノグラフィについて述べる．2.3 節で，SMF ステガノグラフィで初めに提案された基本埋込み方式について述べ，2.4 節でその方式に対して想定される攻撃と，その耐性について述べる．

2.1 SMF の概要[1)~3)]

SMF は，MIDI のシーケンス演奏データのファイル保存形式である．これはディジタル化された楽譜のようなものであり，インターネットで楽曲を発信するための一手段として広く用いられている．

SMF の実体は，ノートイベントがデルタタイムとよばれるイベント間の時間間隔を示す情報に連結されて，1 次元的に配置されたデータ構造である．ノートイベントであるノートオンによって発音された音が，それに対応するノートイベントであるノートオフによって消音される．これら 2 つの MIDI イベントは，ステータスバイト，ノートナンバ，ベロシティの 3 つの情報（各 1 [Byte]）が連結された次のような形式を持つ．

ノートオン：9cH *kk vv*

ノートオフ：8cH *kk vv*

ステータスバイト（9cH または 8cH）の上位 4 [bit] は MIDI イベントの種類を表し，下位 4 [bit] はチャネ

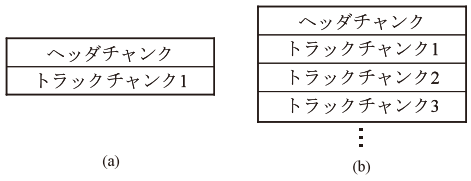

図 1 フォーマット 0/1 の SMF の構造
Fig. 1 The structure of format 0 and 1 SMF.

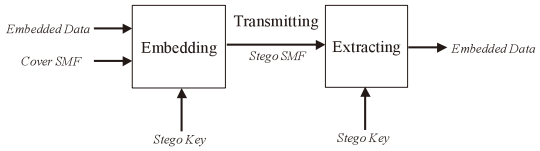

図 2 SMF ステガノグラフィの通信モデル
Fig. 2 The model of SMF steganography.

ルを表す．ノートナンバ（$kk = 0, 1, \ldots, 127$）は音程を表し，鍵盤中央 C を 60 として半音単位で値が割り当てられている．ベロシティ（$vv = 0, 1, \ldots, 127$）は打鍵の速さを表す値で，ノートオン・ベロシティは，一般に音色のリリース・タイムのコントロールに利用される．ただし，ベロシティ0 のノートオンは，ノートオフと同様に消音情報として扱われる．

SMF にはフォーマット 0，1，2 の 3 種類のフォーマットが存在し，フォーマット 0，1 が広く使用されている．フォーマット 0 の SMF は，ヘッダチャンクと，1 つのトラックチャンクで構成され（**図 1** (a)），フォーマット 1 の SMF は，ヘッダチャンクと複数のトラックチャンクで構成される（図 1 (b)）．ヘッダチャンクには，そのファイルのフォーマットや，トラック数などが格納される．トラックチャンクには，ノートイベントなどの実際の演奏データが格納される．

2.2 SMF ステガノグラフィの通信モデル

SMF ステガノグラフィは，送信者が，SMF にまさに伝えたい情報を埋め込むことで，第三者に通信していること自体を秘匿する技術である．通信モデルを**図 2** に示し，説明を行う．まず，送信者が，まさに伝えたい埋込み情報（*Embedded Data*）をフォーマット 0 のカバー SMF（*Cover SMF*）にステゴ鍵（*Stego Key*）を使って埋め込み，ステゴ SMF（*Stego SMF*）を作成する．この処理を埋込み（Embedding）とよぶ．次にステゴ SMF を，情報を伝えたい受信者に対して通信する．これを伝送（Transmitting）とよぶ．最後に，受信者は受信したステゴ SMF から，ステゴ鍵を使って埋込み情報を抽出する．この処理を抽出（Extracting）とよぶ．ここで，伝送中の SMF が埋め込まれているか否かを，判別しようとするステゴ鍵を持たない攻撃者を仮定する．本来 SMF は，音の表現に冗長性を持ち，複数の方法を用いて同じ意味を持つように記述できる．しかし，シーケンサは，その音の並びに規則を与えるため，埋込みを行うことでその規則が崩れる可能性がある．その規則をもとに，攻撃者にカバー SMF かステゴ SMF かを見分けられる可能性がある．

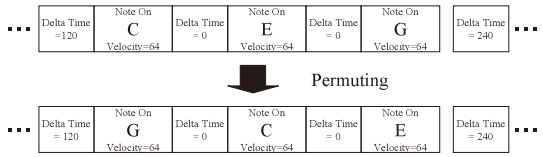

図 3 3 音同時ノートの並べ替え
Fig. 3 Permutation of 3-simulnote.

2.3 基本埋込み方式

本節では，SMF ステガノグラフィで一番初めに提案された埋込み方式（以降，M-0 方式）について，以下に説明する[5]．

SMF で同時に実行されるノートイベントは，デルタタイム 0 で互いに連結されており，MIDI 規格ではそれらの表記順列はとくに規定していない．この同時実行される MIDI イベント群を構成する各々の MIDI イベントの多くは，SMF 内においてどのような順列で表記されていても，演奏データとしての意味は変わらない．つまり，聴覚上はまったく同じに聞こえる．また，並べ替えてもファイルサイズはほとんど変化しない．

そのため，n 音同時ノートは，それに含まれる n 個のノートイベントの順序を並べ替えることで，まったく同じ演奏音で $n!$ 通りの記述方法をとりうる．そこで，同時ノートに含まれるノートイベントの順序のパターンそれぞれに情報を割り当てておき，埋込み情報に応じてノート情報を並べ替えることで，n 音同時ノートには少なくとも $\lfloor \log_2 n! \rfloor$ [bit] の情報を，演奏音を変化させることなく埋め込める（**図 3**）．

また，同時ノート内のノートイベントを順位付けして順列と見なし，この順列をビット列に対応させる．順列とそれに割り当てる情報の対応関係を，ステゴ鍵としてステガノグラフィの送受信者で共有する．**表 1** に，4 音同時ノートまでに対応したステゴ鍵の例を示す．

2.4 想定される攻撃とその耐性

SMF ステガノグラフィでは，カバー SMF とステゴ SMF に見られる特徴の差を考慮することで，SMF がステゴ SMF か否かを見分ける攻撃がある．この攻撃への耐性が重要な評価項目である．そのほかにも，改竄，破壊などの攻撃が考えられるが，本稿では考慮し

表 1 4 音対応ステゴ鍵の例
Table 1 An example of 4-note stegokey.

n音同時ノート	順列⇔ビット列	n音同時ノート	順列⇔ビット列
2音	12 ⇔ 0 21 ⇔ 1	4音	2314 ⇔ 1000 2341 ⇔ 1001 2413 ⇔ 1010 2431 ⇔ 1011 3124 ⇔ 1100 3124 ⇔ 1100 3142 ⇔ 1101 3214 ⇔ 1110 3241 ⇔ 1111 3412 ⇔ 0000 3421 ⇔ 0001 4123 ⇔ 0010 4132 ⇔ 0011 4213 ⇔ 0100 4231 ⇔ 0101 4312 ⇔ 0110 4321 ⇔ 0111
3音	123 ⇔ 00 132 ⇔ 01 213 ⇔ 10 231 ⇔ 11 312 ⇔ 00 321 ⇔ 01		
4音	1234 ⇔ 0000 1243 ⇔ 0001 1324 ⇔ 0010 1342 ⇔ 0011 1423 ⇔ 0100 1432 ⇔ 0101 2134 ⇔ 0110 2143 ⇔ 0111		

表 2 インターネット上の SMF に見られる特徴
Table 2 Characteristics of SMFs downloaded from the Internet.

特徴 1: 同時ノートは，ノートオフが先にノートオンが後にまとめて記述される．
特徴 2: 同時ノート中のノートオンは，同じチャネルごとにまとめて記述される．
特徴 3: 同時ノートはノートナンバに対して昇順に記述される．

ない．文献 6) は，インターネット上の国内外の主要な SMF 投稿サイトから収集してきた SMF 19,069 曲のうち，フォーマット 0 の SMF 3,643 曲の同時ノートから，**表 2** の特徴を見つけ，これをもとに M-0 方式で埋め込んだステゴ SMF を解析した．その結果，M-0 方式で埋め込んだ 97 [%] のステゴ SMF の埋込みが検出できることを示している．以降，表 2 の特徴 1 と特徴 2 の少なくとも一方を満たすか否かを調べる解析を解析 1 と定義し，少なくとも一方を満たす場合に「解析 1 に対して耐性がある」ということにする．ただし，文献 6) によると，特徴 3 を満たす SMF は非常に少ないことから，本稿では特徴 3 は考慮しない．また，文献 6) では，解析 1 に耐性を持たせるために，特徴 1 または特徴 2 を満たす埋込み方法 1，2（以降 M-1 方式，M-2 方式）が提案されている．M-1 方式では，同時ノート中でノートオフを先に，ノートオンを後にまとめ，ノートオフとノートオンのまとまりの中で，ノートイベントを並べ替えることで埋め込んでいる．M-2 方式では，同時ノート中で同じチャネルごとにまとめ，チャネルごとのまとまりを並べ替えることで埋め込み，さらに同じチャネルのまとまりの中で，ノートイベントを並べ替えることで埋め込んでいる．なお，すでに述べたように，特徴 3 を満たす SMF はほとんどなく，SMF が特徴 3 を持つこと自体が検出の手がかりとなる可能性があるので，特徴 3 を満たす埋込み方式は提案されていない．M-1 方式，M-2 方式は，M-0 方式と比較し，埋め込む同時ノートの数が減少するため埋込み率が低下する．

3. SMF 編集ソフトウェアの特徴を考慮した埋込み手法の提案

一般的に SMF はシーケンサにより編集・生成されるため，表 2 で示した特徴は，シーケンサが残していると考えられる．そこで本章では，シーケンサが SMF に残す特徴を考慮して埋め込むことで，シーケンサの特徴を利用した解析に対して耐性のある埋込み手法を提案する．

以下，3.1 節で，シーケンサの特徴を考慮した一般的な埋込み手法を提案し，3.2 節で提案手法を基に具体的な埋込み方式を提案する．また，3.3 節では 3.2 節の埋込み方式をさらに拡張した方式である M-∗ 方式を提案する．

3.1 編集ソフトウェアの特徴を考慮した埋込み手法の提案

本節では，シーケンサ固有の特徴を満たすように SMF に埋め込む埋込み手法を提案する．文献 6) で提案された方式は，インターネット上の SMF に見られる特徴を考慮していたが，提案方式では，シーケンサが SMF に残す特徴を考慮するという点で異なる．この埋込み手法により埋め込まれたステゴ SMF は，固有のシーケンサの特徴を満たしているため，そのシーケンサによって生成された SMF と見分けがつかないと考えられる．つまりシーケンサの特徴を考慮した解析に対して耐性を持つことが期待できる．

いま，シーケンサ X_1，X_2，...，X_n を考える．これらのシーケンサが SMF に残す特徴をそれぞれ特徴 X_1，特徴 X_2，...，特徴 X_n とし，それぞれの特徴を満たすように埋め込む方式をそれぞれ M-X_1方式，M-X_2方式，...，M-X_n方式とする．この方式に対する解析として，SMF が特徴 X_1，特徴 X_2，...，特徴 X_n の少なくとも 1 つを満たすかを調べる解析を考え，少なくとも 1 つの特徴を満たすとき，提案方式はこの解析に対して耐性を持つと定義する．なお，この解析は，3.2 節での解析 2 と対応している．

図 4 に，提案方式の概要の図を示し，埋込み，抽出の際の手順を述べる．図 4 において，Checking 関数では，シーケンサの特徴を持たせつつ埋込み可能な SMF か否かをチェックし，埋込み不可能な SMF の

表 3 調査したシーケンサ
Table 3 Analyzed sequencers.

呼び方	シーケンサ名	対応OS	バージョン	開発元
シーケンサA	CubaseVST 5	Windows 95/98/2000	5.1	Steinberg
シーケンサB	XGworks version4.0	Windows 95/98/NT4.0	4.0.4	YAMAHA
シーケンサC	レコンポーザ95	Windows 95/NT4.0	2.2	カモンミュージック
シーケンサD	SingerSongWriter 6.0 VS	Windows 95/98/Me/ 2000/NT4.0	6.00.6	インターネット
シーケンサE	Logic Platinum 5	Windows 98/98 SE/Me 2000/XP	5.01	emagic

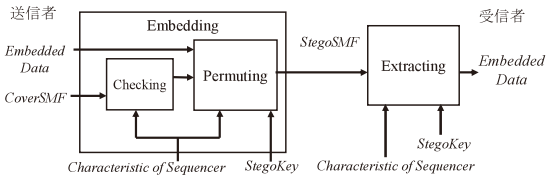

図 4 提案手法の概要
Fig. 4 Proposed method.

場合は埋込みを行わず，処理を中止する．これは，同時ノートの並びによっては，シーケンサの特徴を持たせた場合，音が変化する場合がありうるためである．Permuting 関数では，シーケンサの特徴を持たせつつ，同時ノート中の埋込み可能な部分に対し，ステゴ鍵を参照して並べ替えの処理を行う．Extracting 関数では，どの方式で埋め込まれているかを確認し，ステゴ鍵を参照することで，同時ノート中の埋め込まれている部分から埋込み情報を抽出する．以下に，埋込み・抽出の手順を示す．

【準備】
あらかじめ送信者と受信者は，シーケンサの特徴とステゴ鍵の情報を共有する．

【埋込み】
埋込み手順 1. Checking 関数で，シーケンサの特徴を持たせつつ埋め込める SMF かどうか判定する．
埋込み手順 2. 埋め込める SMF の場合，Permuting 関数で，シーケンサの特徴を持たせるように，同時ノート中のノートオンにステゴ鍵を参照して埋め込む．

【抽出】
Extracting 関数で，あらかじめ共有しておいたシーケンサの特徴とステゴ鍵を参照して埋込み情報を抽出する．

3.2 代表的な編集ソフトウェアの特徴を考慮した埋込み方式

本節では，3.1 節で提案した手法に基づき，現在広く用いられていると考えられる代表的なシーケンサの特徴を用いて，具体的な埋込み方式を提案する．**表 3** に，本稿で考察対象とするシーケンサ[4] を示す．表 3 の各シーケンサが SMF に残す特徴を，それぞれ特徴 A，特徴 B，特徴 C，特徴 D，特徴 E とする．各シーケンサがフォーマット 0 の SMF に残す特徴を**表 4** にまとめ，フォーマット 1 の SMF に残す特徴を，**表 5** にまとめた．表中では，同時ノートが項目を満たす場合を “◯” と表記した．また，シーケンサ E ではフォーマット 0 の SMF が作成できないため，表 4 では表記しない．

図 5，**図 6** を用いて，表 4，表 5 の説明をする．

表 4 の「オフが先，オンが後」とは，同時ノート III において，ノートオフ (8)〜(14) が先，ノートオン (15)，(16) が後に記述された状態を指す．また，「オンが先，オフが後」は，この例とは逆の状態を指す．「チャネルごとにまとまり，オフが先，オンが後」とは，ノートイベント (17)〜(19) や (20)，(21) のように，同じチャネルのノートオンとノートオフがまとまり，かつそれぞれでノートオフが先，ノートオンが後になる状態を指す．

表 4 の「ノートオンのチャネルごとのまとまり」かつ「チャネルごとにまとまる」とは，(1) と (2)，(5)〜(7) がチャネルごとにまとまる状態を指す．「ノートオフのチャネルごとのまとまり」かつ「チャネルごとにまとまらない」は，同時ノート I，II の (1)〜(7) のノートオンに対応するノートオフが，同時ノート III の (8)〜(14) で，チャネルに関して逆順に並んでいる状態を指す．

表 4 の「ノートオンの最小単位でのノートの並び」かつ「任意」は，同時ノート I の (1) と (2)，同時ノート II の (5)〜(7) のような，チャネルごとにまとまったノートオンの固まりの中でのノートの並び方が，SMF 作成者によって自由に決められることを指す．「ノートオフの最小単位でのノートの並び」かつ「対応するオンのノートの並びと逆順」は，同時ノート II のノートオン (5)〜(7) に対応する同時ノート III のノートオフ (8)〜(10) が，逆順に並んでいる状態を指す．

表 5 の「トラック内のチャネルの数」かつ「単一」

表 4 シーケンサがフォーマット 0 の SMF に残す特徴
Table 4 Characteristics of sequencers for format 0 SMFs.

			A	B	C	D
ノートオンとノートオフのまとまり方	オンが先 ・オフが後		○			
	オフが先・オンが後 (従来の特徴1)			○		○
	チャネルごとにまとまり，オフが先・オンが後				○	
ノートオンのチャネルごとのまとまり	チャネルごとにまとまる	昇順		○	○	○
	チャネルごとにまとまらない		○			
ノートオフのチャネルごとのまとまり	チャネルごとにまとまる	昇順			○	
	チャネルごとにまとまらない	対応するオンのチャネルの並びと同順				○
		対応するオンのチャネルの並びと逆順	○	○		
ノートオンの最小単位でのノートの並び	昇順					
	任意		○	○	○	○
ノートオフの最小単位でのノートの並び	昇順					
	対応するオンのノートの並びと同順				○	○
	対応するオンのノートの並びと逆順		○	○		

表 5 シーケンサがフォーマット 1 の SMF に残す特徴
Table 5 Characteristics of sequencers for format 1 SMFs.

				A	B	C	D	E
トラック内のチャネルの数	単一				○	○	○	
	複数			○				○
トラック内のノートオン・ノートオフのまとまり方	オンが先・オフが後							
	オフが先・オンが後			○	○	○	○	○
ノートオンのチャネルごとのまとまり	単一チャネル				○	○	○	
	複数チャネル	チャネルごとにまとまる	昇順					○
		チャネルごとにまとまらない	任意	○				
ノートオフのチャネルごとのまとまり	単一チャネル				○	○	○	
	複数チャネル	チャネルごとにまとまる	昇順					○
		チャネルごとにまとまらない	対応するオンのチャネルの並びと逆順	○				
ノートオンの最小単位でのノートの並び	昇順							○
	任意			○	○	○	○	
ノートオフの最小単位でのノートの並び	昇順							○
	対応するオンのノートの並びと同順					○	○	
	対応するオンのノートの並びと逆順			○	○			

とは，1 つのトラックチャンク内には 1 つの種類のチャネルしか存在しない状態を指す．

以降，SMF について，表 4 と表 5 で示した特徴 A，特徴 B，特徴 C，特徴 D，特徴 E のうちの少なくとも 1 つを満たすか否かを調べる解析を解析 2 と定義し，少なくとも 1 つを満たすとき「解析 2 に対して耐性がある」と定義する．つまり，現実に存在するシーケンサが SMF に残す特徴を持たない SMF をステゴ SMF と見なす解析を考える．調査によって得られた表 4 と表 5 の特徴を用い，解析 2 に対して耐性を持つ具体的な埋込み方式を提案する．解析者は，あるSMF が持つ同時ノートが，特徴 A，特徴 B，特徴 C，特徴 D，特徴 E のいずれも満たしていない場合，ステゴ SMF と判断する．そのため，その特徴を崩さないように埋め込めば，解析者は埋め込まれているかどうかを，同時ノートを見ることでは判断できない．この際，同時ノートの特徴からシーケンサを推定し，そのシーケンサにいったん SMF を入力し，出力することで SMF の特徴の変化を調べ，変化すればステゴ SMF であるとする解析に対しても，提案方式は耐性がある．実際，本節の提案方式で埋め込んだステゴ SMF の場合，シーケンサの出力を観察し，冗長な部分にのみ埋

	Meas	Ch	Event	note No	Vel	
同時ノート I	3:1:000	1	N_On	67(G4)	64	(1)
	3:1:000	1	N_On	60(C4)	60	(2)
	3:1:000	2	N_On	79(G5)	80	(3)
	3:1:000	3	N_On	72(C5)	75	(4)
同時ノート II	4:1:000	1	N_On	64(E4)	64	(5)
	4:1:000	1	N_On	55(G3)	64	(6)
	4:1:000	1	N_On	59(B3)	64	(7)
同時ノート III	5:1:000	1	N_Off	59(B3)	64	(8)
	5:1:000	1	N_Off	55(G3)	64	(9)
	5:1:000	1	N_Off	64(E4)	64	(10)
	5:1:000	3	N_Off	72(C5)	64	(11)
	5:1:000	2	N_Off	79(G5)	64	(12)
	5:1:000	1	N_Off	60(C4)	64	(13)
	5:1:000	1	N_Off	67(G4)	64	(14)
	5:1:000	1	N_On	52(E3)	64	(15)
	5:1:000	2	N_On	71(B4)	74	(16)

図 5 特徴 B を満たす同時ノートの例
Fig. 5 An example of characteristic B.

	Meas	Ch	Event	note No	Vel	
同時ノート IV	5:1:000	1	N_Off	55(G3)	64	(17)
	5:1:000	1	N_Off	64(E4)	64	(18)
	5:1:000	1	N_On	52(E3)	64	(19)
	5:1:000	2	N_Off	79(G5)	64	(20)
	5:1:000	2	N_On	71(B4)	74	(21)
	5:1:000	3	N_Off	72(C5)	60	(22)

図 6 特徴 C を満たす同時ノートの例
Fig. 6 An example of characteristic C.

め込んでいるため，ステゴ SMF がシーケンサ固有の特徴を満たすことから変化は現れないと考えられるからである．提案方式を，それぞれ M-A 方式，M-B 方式，M-C 方式，M-D 方式とする．ただし，シーケンサ E で作成した SMF は，同時ノート内のノートイベントの並びが一意に定まる．そのため，同時ノート内のノートイベントの並べ替えが行えないため埋め込めない．

表 4 と**図 7** を用い，フォーマット 0 の SMF に対する M-B 方式の埋込み手順の例を以下に説明する．表 4 から，特徴 B はノートオフが先，ノートオンが後にまとまり，ノートオンはチャネルごとにまとまり，ノートオフは対応するノートオンの並びと逆順に整列する．そのため，特徴 B を満たしつつ並べ替え可能なノートは，同じチャネルごとのノートオンのみである．図 7 に，M-B 方式で埋め込む例を示す．図 7 (a) の SMF に対し，まず M-B 方式の特徴を満たすよう，まず，ノートオフを先に，ノートオンを後にまとめ，ノートオンのチャネルに関して昇順に整列すると図 7 (b) になる．

Meas	Ch	Event	note No	Vel
3:1:000	1	N_On	67(G4)	64
3:1:000	3	N_On	72(C5)	75
3:1:000	2	N_On	79(G5)	80
3:1:000	1	N_On	60(C4)	60
4:1:000	1	N_On	55(G3)	64
4:1:000	1	N_On	64(E4)	64
4:1:000	1	N_On	59(B3)	64
5:1:000	1	N_Off	59(B3)	64
5:1:000	1	N_Off	60(C4)	64
5:1:000	1	N_On	52(E3)	64
5:1:000	3	N_Off	72(C5)	64
5:1:000	1	N_Off	67(G4)	64
5:1:000	2	N_Off	79(G5)	64
5:1:000	2	N_On	71(B4)	74
5:1:000	1	N_Off	55(G3)	64
5:1:000	1	N_Off	64(E4)	64

(a)

Meas	Ch	Event	note No	Vel
3:1:000	1	N_On	67(G4)	64
3:1:000	1	N_On	60(C4)	60
3:1:000	2	N_On	79(G5)	80
3:1:000	3	N_On	72(C5)	75
4:1:000	1	N_On	64(E4)	64
4:1:000	1	N_On	55(G3)	64
4:1:000	1	N_On	59(B3)	64
5:1:000	1	N_Off	59(B3)	64
5:1:000	1	N_Off	55(G3)	64
5:1:000	1	N_Off	64(E4)	64
5:1:000	3	N_Off	72(C5)	64
5:1:000	2	N_Off	79(G5)	64
5:1:000	1	N_Off	60(C4)	64
5:1:000	1	N_Off	67(G4)	64
5:1:000	1	N_On	52(E3)	64
5:1:000	2	N_On	71(B4)	74

(b)

Meas	Ch	Event	note No	Vel
3:1:000	1	N_On	60(C4)	60
3:1:000	1	N_On	67(G4)	64
3:1:000	2	N_On	79(G5)	80
3:1:000	3	N_On	72(C5)	75
4:1:000	1	N_On	59(B3)	64
4:1:000	1	N_On	64(E4)	64
4:1:000	1	N_On	55(G3)	64
5:1:000	1	N_Off	59(B3)	64
5:1:000	1	N_Off	55(G3)	64
5:1:000	1	N_Off	64(E4)	64
5:1:000	3	N_Off	72(C5)	64
5:1:000	2	N_Off	79(G5)	64
5:1:000	1	N_Off	60(C4)	64
5:1:000	1	N_Off	67(G4)	64
5:1:000	1	N_On	52(E3)	64
5:1:000	2	N_On	71(B4)	74

(c)

Meas	Ch	Event	note No	Vel
3:1:000	1	N_On	60(C4)	60
3:1:000	1	N_On	67(G4)	64
3:1:000	2	N_On	79(G5)	80
3:1:000	3	N_On	72(C5)	75
4:1:000	1	N_On	59(B3)	64
4:1:000	1	N_On	64(E4)	64
4:1:000	1	N_On	55(G3)	64
5:1:000	1	N_Off	55(G3)	64
5:1:000	1	N_Off	64(E4)	64
5:1:000	1	N_Off	59(B3)	64
5:1:000	3	N_Off	72(C5)	64
5:1:000	2	N_Off	79(G5)	64
5:1:000	1	N_Off	67(G4)	64
5:1:000	1	N_Off	60(C4)	64
5:1:000	1	N_On	52(E3)	64
5:1:000	2	N_On	71(B4)	74

(d)

図 7 M-B 方式による埋込み手順
Fig. 7 Embedding procedure of M-B.

次に，冗長な部分である同じチャネルごとのノートオンを並べ替え，情報を埋め込むと，図 7 (c) になる．最後にノートオンの並びに従い，ノートオフを並べ替えると図 7 (d) になる．

さらに，本節の提案方式は，上記で解析したシーケンサに限らず，SMF に残すノートの並びに関する特徴について冗長性があるようなシーケンサであれば適用できる．

3.3 M-∗ 方式への拡張

3.1 節および 3.2 節で示したように，複数のシーケンサに対して，それぞれ埋込み方式を提案できる．本節では，ある SMF に対し，解析に対する耐性が同じである複数の埋込み方式が適用できる場合には，最も埋込み可能情報量の高い埋込み方式を採用するように拡張する．この採用方法によって 3.2 節で提案した埋込み方式の中から埋込み方式を選択して埋め込む方式を M-∗ 方式と定義する．ここで，解析 1 と解析 2 の両方に対して耐性のある方式の中で，最も埋込み可能情報量の高い埋込み方式を採用する方式を M-∗I 方式と定義する．また，解析 2 に対して耐性のある方式の中で，最も埋込み可能情報量の高い埋込み方式を採用

する方式を M-∗II 方式と定義する．

フォーマット 0 の SMF において，特徴 B，特徴 C，特徴 D が表 2 の特徴 1，特徴 2 を満たし，特徴 A は表 2 の特徴 1，特徴 2 のいずれも満たさないため，M-B 方式，M-C 方式，M-D 方式を用いた M-∗I 方式が提案できる．また，すべての方式が，特徴 A，特徴 B，特徴 C，特徴 D のいずれかを満たすことから，解析 2 に対し耐性があるため，M-A 方式，M-B 方式，M-C 方式，M-D 方式の中で最も埋込み率の高い埋込み方式を採用する M-∗II 方式が提案できる．

フォーマット 1 の SMF においては，特徴 A，特徴 B，特徴 C，特徴 D が表 2 の特徴 1 を満たすため，M-∗I 方式と M-∗II 方式の両方において，M-A 方式，M-B 方式，M-C 方式，M-D 方式の中で最も埋込み率の高い埋込み方式を採用する．

以下に，M-∗ 方式の準備と，埋込み・抽出の手順を示す．

【準備】

あらかじめ，送信者と受信者は，ステゴ鍵と複数の埋込み方式の候補の情報を共有する．

【埋込み】

埋込み手順 1. 複数の埋込み方式に関し，Checking 関数で，どのシーケンサの特徴を持たせつつ埋め込み可能な SMF なのかを調べる．

埋込み手順 2. 適用できる埋込み方式の中で最も埋込み可能情報量の高い埋込み方式を採用し，埋め込む．

【抽出】

あらかじめ共有しておいた埋込み方式の候補とステゴ鍵を参照し，各埋込みの候補に対し，抽出処理を行う．このうち，意味のある情報が抽出できた場合に抽出成功と見なす．

4. 考　　察

本章では，提案方式についての考察を行う．以降，4.1 節で各フォーマットにおける編集ソフトウェアの特徴を考慮した埋込み方式の性能評価を行い，4.2 節で，M-∗ 方式の性能評価を行う．

3.2 節，3.3 節で提案した埋込み方式の性能評価を行うため，フォーマット 0 の SMF とフォーマット 1 の SMF に対する埋込み率（カバー SMF に対する埋込み可能情報量の比率）を実験により計測した．評価にあたっては，実際にシーケンサを利用している多くのユーザにより作成された SMF が評価に適していると考え，計測対象の SMF として国内外のインターネット上の SMF 投稿サイトから SMF 18,699 曲をダウンロードしたものを用いた．このうち，フォーマット 0 の SMF は 3,643 曲であり，フォーマット 1 の SMF は 15,056 曲である．また，埋込みには 8 音対応ステゴ鍵の使用を仮定した．また，これらの SMF において，式 (1) で定義される埋込み率を値にとる確率変数 X に対して，その期待値（以降，平均埋込み率とよぶ）と分散を求めた．フォーマット 0，フォーマット 1 の SMF それぞれに対する各方式の平均埋込み率，分散，平均埋込み可能情報量，解析 1，解析 2 に対する耐性を，**表 6**，**表 7** に示す．表 6，表 7 では，該当する解析に耐性のある方式の場合を “◯” とし，該当する方式で生成したステゴ SMF が，各解析で検出できる可能性がある場合 “×” と表記した．また，フォーマット 0 の SMF に対する各埋込み方式による埋込み率の分布図を**図 8**〜**図 15** に示し，フォーマット 1 の SMF に対する埋込み率の分布図を**図 16**〜**図 22** に示す．ここで各分布図において，縦軸は埋込み可能 SMF 数，横軸は埋込み率である．ただし，フォーマット 0

表 6 フォーマット 0 の SMF への平均埋込み率
Table 6 Average embedding rate of format 0 SMFs.

		平均埋込み率[%]	分散	平均埋込み可能容量[bit]	埋込み可能なSMF[曲]	解析 1	解析 2
既存の方式	M-0方式	1.73	0.923	6,236	3,626 (99.5 %)	×	×
	M-1方式	1.60	0.905	5,649	3,270 (89.8 %)	○	×
	M-2方式	1.41	0.502	4,977	3,553 (97.5 %)	○	×
提案方式	M-A方式	0.69	0.238	1,128	806 (22.1 %)	×	○
	M-B方式	0.37	0.090	1,290	2,467 (67.7 %)	○	○
	M-C方式	0.37	0.082	1,333	2,697 (74.0 %)	○	○
	M-D方式	0.37	0.090	1,290	2,467 (67.7 %)	○	○
	M-∗I方式	0.37	0.087	1,338	2,787 (76.5 %)	○	○
	M-∗II方式	0.51	0.142	1,561	2,816 (77.3 %)	×	○

(括弧の中は3,643曲中の割合)
(○は耐性あり，×は耐性なし)
(平均埋込み可能容量は小数点以下切捨て)

表 7 フォーマット 1 の SMF への平均埋込み率
Table 7 Average embedding rate of format 1 SMFs.

		平均埋込み率[%]	分散	平均埋込み可能容量[bit]	埋込み可能なSMF[曲]	解析 1	解析 2
既存の方式	M-0方式	1.004	0.404	3,222	14,525 (96.5 %)	×	×
	M-1方式	0.854	0.358	2,926	12,142 (80.6 %)	○	×
	M-2方式	0.998	0.395	3,206	14,524 (96.5 %)	○	×
提案方式	M-A方式	0.484	0.104	1,642	11,376 (75.6 %)	○	○
	M-B方式	0.471	0.095	1,615	11,769 (78.2 %)	○	○
	M-C方式	0.471	0.095	1,610	11,633 (77.3 %)	○	○
	M-D方式	0.471	0.095	1,610	11,633 (77.3 %)	○	○
	M-∗I方式	0.485	0.104	1,667	11,817 (78.5 %)	○	○
	M-∗II方式	0.485	0.104	1,667	11,817 (78.5 %)	○	○

(括弧の中は15,056曲中の割合)
(○は耐性あり，×は耐性なし)
(平均埋込み可能容量は小数点以下切捨て)

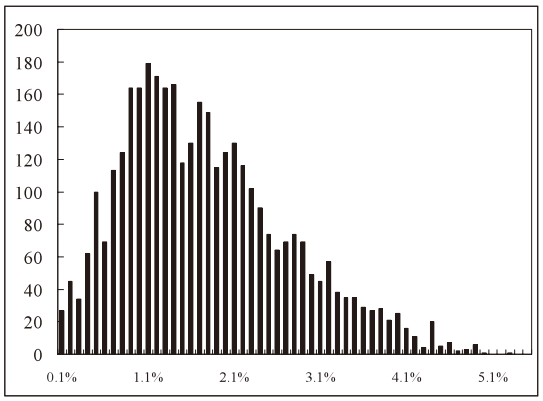

図 8 フォーマット 0 の SMF に M-0 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 8 Distribution of embedding rate of format 0 SMFs in method M-0, where the vertical axis means the number of music and the horizontal axis means embedding rates.

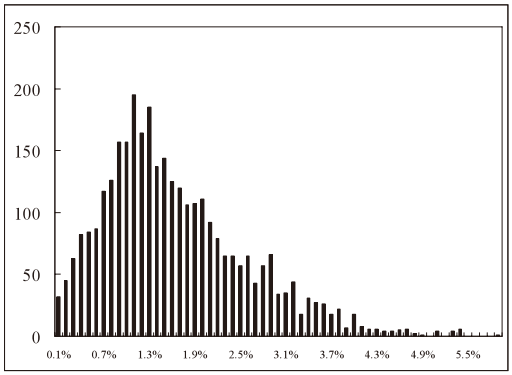

図 9 フォーマット 0 の SMF に M-1 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 9 Distribution of embedding rate of format 0 SMFs in method M-1, where the vertical axis means the number of music and the horizontal axis means embedding rates.

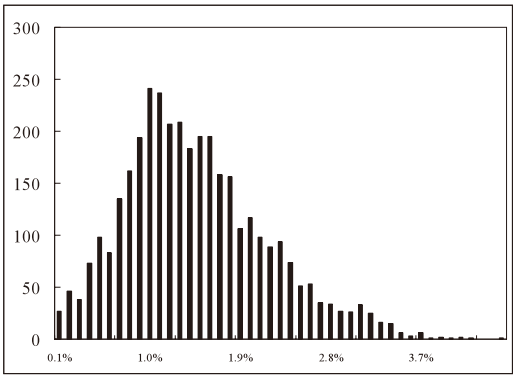

図 10 フォーマット 0 の SMF に M-2 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 10 Distribution of embedding rate of format 0 SMFs in method M-2, where the vertical axis means the number of music and the horizontal axis means embedding rates.

の SMF への埋込み率計測実験の結果において M-B 方式と M-D 方式は同じ計測アルゴリズムを用いたため，同じ図にまとめた．同様に，フォーマット 1 の SMF への埋込み率計測実験の結果では，M-C 方式と M-D 方式，M-∗I 方式と M-∗II 方式がそれぞれ同じ結果になるため，同じ図にまとめた．

$$\text{埋込み率 [\%]} = \frac{\text{埋込み可能情報量 [bit]}}{\text{カバー SMF のサイズ [bit]}} \times 100 \qquad (1)$$

4.1 M-A，M-B，M-C，M-D 方式の性能評価

表 6，図 8〜図 13 より，フォーマット 0 の SMF に対して M-A 方式，M-B 方式，M-C 方式，M-D 方式を適用した場合，既存の方式を適用した場合と比較して埋込み率が低下していることが分かる．これは，提案方式が既存の方式と比較し，埋込み可能な同時ノートの数が少ないからだと考えられる．また，M-A 方式による埋込みは，解析 1 の耐性がないことが分かる．

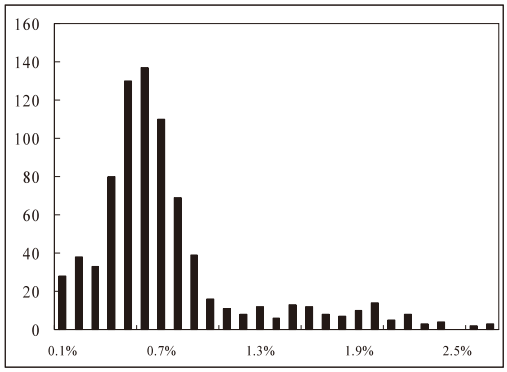

図 11 フォーマット 0 の SMF に M-A 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）

Fig. 11 Distribution of embedding rate of format 0 SMFs in method M-A, where the vertical axis means the number of music and the horizontal axis means embedding rates.

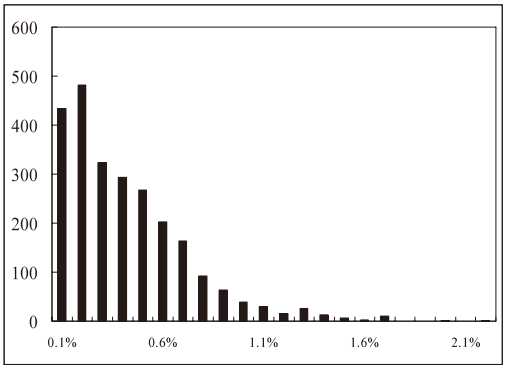

図 12 フォーマット 0 の SMF に M-B 方式，M-D 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）

Fig. 12 Distribution of embedding rate of format 0 SMFs in method M-B or method M-D, where the vertical axis means the number of music and the horizontal axis means embedding rates.

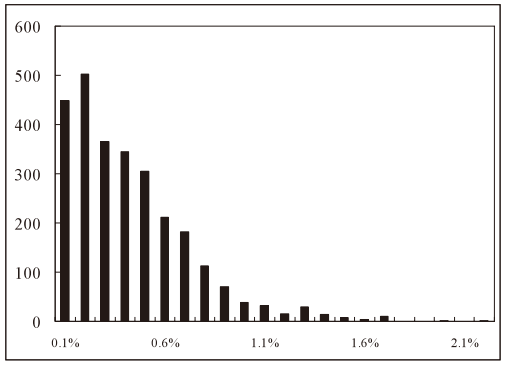

図 13 フォーマット 0 の SMF に M-C 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）

Fig. 13 Distribution of embedding rate of format 0 SMFs in method M-C, where the vertical axis means the number of music and the horizontal axis means embedding rates.

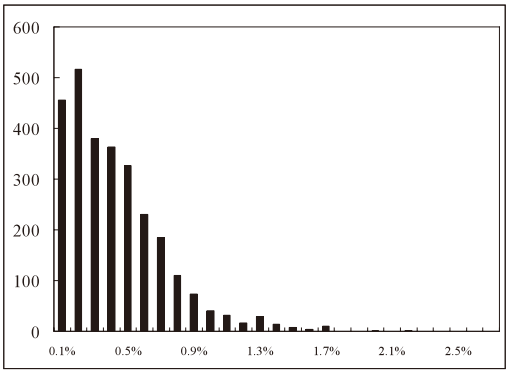

図 14 フォーマット 0 の SMF に M-∗I 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）

Fig. 14 Distribution of embedding rate of format 0 SMFs in method M-∗I, where the vertical axis means the number of music and the horizontal axis means embedding rates.

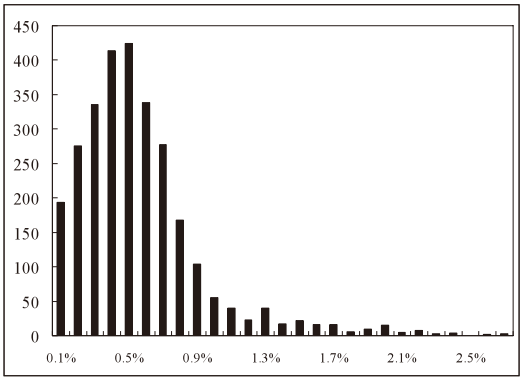

図 15 フォーマット 0 の SMF に M-∗II 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）

Fig. 15 Distribution of embedding rate of format 0 SMFs in method M-∗II, where the vertical axis means the number of music and the horizontal axis means embedding rates.

これは，シーケンサ A がフォーマット 0 の SMF に残す特徴が，表 2 で示されるインターネット上の SMF に見られる特徴と異なるためであるといえる．提案方式は，同時ノート中のノートオフに埋め込めず，さらに M-B 方式，M-C 方式，M-D 方式に関しては，チャネルごとのノートオンに対してのみ埋め込める．比較的 M-A 方式の埋込み率が高いのは，ノートオンに対し，チャネルにかかわらず埋め込めるためだと考えられる．

表 7，図 16〜図 21 より，フォーマット 1 の SMF に対して M-A 方式，M-B 方式，M-C 方式，M-D 方式を適用した場合，既存の方式を適用した場合と比較して 1/2 程度に埋込み率が低下しているが，フォーマット 0 の SMF に対して適用した場合ほどの大きな低下

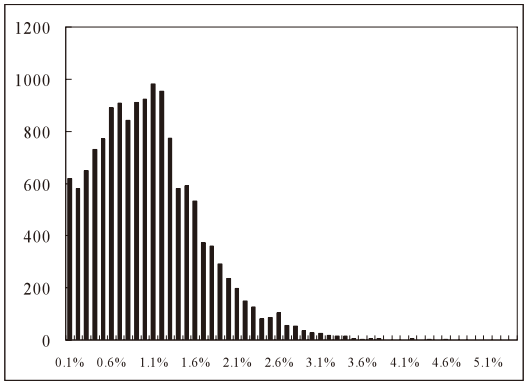

図 16 フォーマット 1 の SMF に M-0 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 16 Distribution of embedding rate of format 1 SMFs in method M-0, where the vertical axis means the number of music and the horizontal axis means embedding rates.

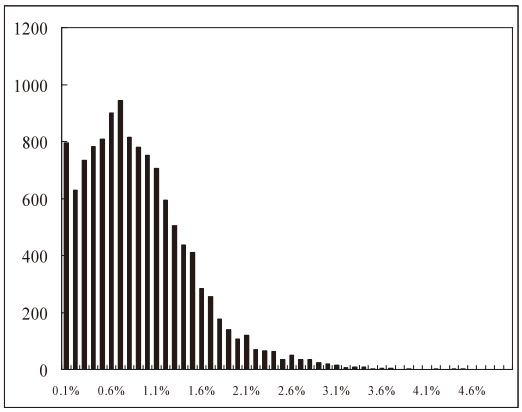

図 17 フォーマット 1 の SMF に M-1 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 17 Distribution of embedding rate of format 1 SMFs in method M-1, where the vertical axis means the number of music and the horizontal axis means embedding rates.

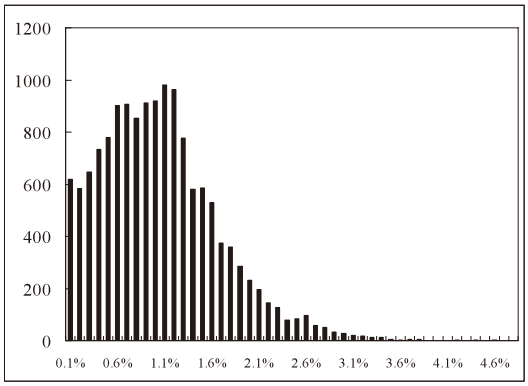

図 18 フォーマット 1 の SMF に M-2 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 18 Distribution of embedding rate of format 1 SMFs in method M-2, where the vertical axis means the number of music and the horizontal axis means embedding rates.

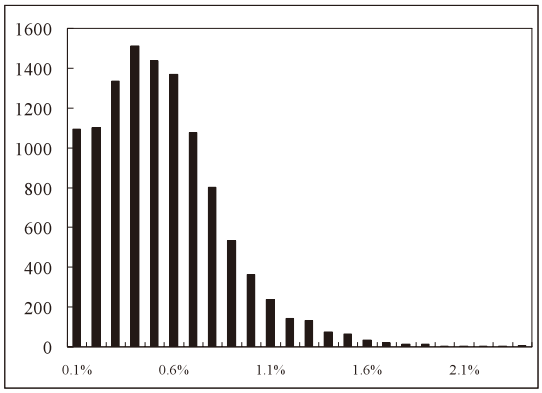

図 19 フォーマット 1 の SMF に M-A 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 19 Distribution of embedding rate of format 1 SMFs in method M-A, where the vertical axis means the number of music and the horizontal axis means embedding rates.

は見られなかった．これは，フォーマット 1 の SMF は，1 つのチャンクの中に 1 つのチャネルが格納されることで，チャネルが違うノートが離れている傾向があるためであると考えられる．

表 6 と表 7 より，フォーマット 1 の M-A 方式は，フォーマット 0 の M-A 方式と比較して埋込み率が低かったが，M-B 方式，M-C 方式，M-D 方式に関しては埋込み率が高くなった．これは，フォーマット 1 のサンプルが，全体的に同時ノートの数が多く構成されていたからであると考えられる．

4.2 M-∗ 方式の性能評価

表 6 より，M-∗I 方式の平均埋込み率は，これを構成する方式による埋込み率と比較して変化はないが，埋込み可能 SMF が 3〜9 [%] 増加したことが分かる．これにより，この方式を用いると，解析に対する耐性と平均埋込み率を保ちつつ，埋込み可能 SMF を増やせるといえる．また，M-∗II は，M-∗I と比較して，埋込み可能 SMF はあまり変化はなかったが，平均埋込み率が 0.14 [%] 増加した．しかし，埋め込む際に M-A 方式を採用した場合，解析 1 により検出できる可能性がある．これにより，この方式を用いると，解析 1 に対する耐性が下がるものの，平均埋込み率と埋込み可能 SMF の増加が期待できるといえる．

表 7 より，M-∗I，M-∗II 方式は，埋込み可能 SMF に関して，最大に埋め込めた M-A 方式と比較して 0.3 [%] 程度増加したことが分かる．

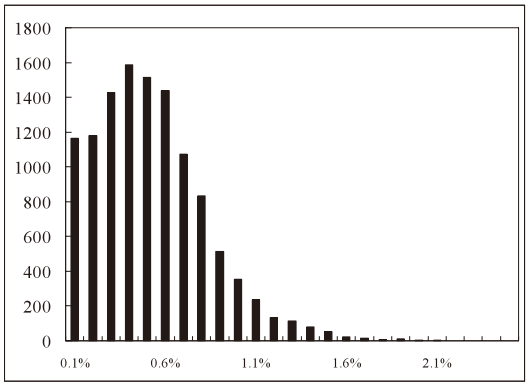

図 20 フォーマット 1 の SMF に M-B 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 20 Distribution of embedding rate of format 1 SMFs in method M-B, where the vertical axis means the number of music and the horizontal axis means embedding rates.

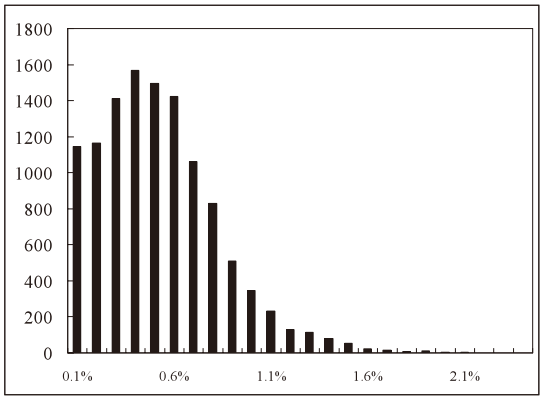

図 21 フォーマット 1 の SMF に M-C 方式，M-D 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 21 Distribution of embedding rate of format 1 SMFs in method M-C or method M-D, where the vertical axis means the number of music and the horizontal axis means embedding rates.

5. ま と め

本稿では，シーケンサが SMF に残す特徴を調査し，シーケンサが SMF に残す特徴を考慮した埋込み方式を提案した．文献 6) の方式は，インターネット上の SMF に見られる特徴が，シーケンサの影響を受けることを考慮し，インターネット上の SMF に見られる特徴を考慮した埋込み方式を提案していた．本稿での提案方式は，文献 6) の方式と比較し，シーケンサが SMF に残す特徴を考慮することで，現実に存在している SMF の持つ特徴をより正確に再現しているという点で，より秘匿性の高い方式であるといえる．また，

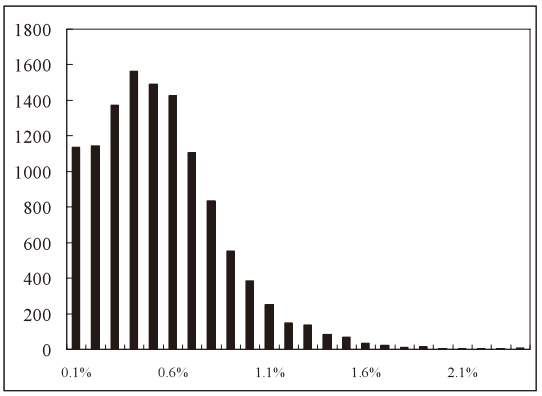

図 22 フォーマット 1 の SMF に M-∗I 方式，M-∗II 方式を適用した場合の埋込み率の分布（ただし縦軸は曲数，横軸は埋込み率を表す）
Fig. 22 Distribution of embedding rate of format 1 SMFs in method M-∗I or method M-∗II, where the vertical axis means the number of music and the horizontal axis means embedding rates.

フォーマット 0 とフォーマット 1 の SMF を用い，提案方式の埋込み性能を評価した．その結果，既存の方式はフォーマット 0 に対する埋込み率と比較し，フォーマット 1 に対する埋込み率は大きく減少したが，提案方式は，フォーマット 1 の SMF に対してもフォーマット 0 と同程度の解析に対する埋込み率と高い耐性を保ちつつ埋め込めることを示した．インターネット上の SMF 投稿サイトから無作為にダウンロードした SMF において，フォーマット 1 の SMF が高い割合を占めることから，提案方式は多くの SMF に対する埋込み方式として，高い秘匿性を保ちつつ多くの情報を埋め込むことができる方式であるといえる．また，M-∗ 方式について性能評価を行い，フォーマット 0 の SMF において，解析に対する耐性と平均埋込み率を保ちつつ，埋込み可能 SMF 数の増加が期待できる方式と，解析に対する耐性は下がるが，平均埋込み率と埋込み可能 SMF 数の両方の増加が期待できる方式の 2 つを提案した．

謝辞 本研究の一部は，文部科学省科学研究費補助金特定領域研究 13224040（松本勉）の支援を受けて行われた．

参 考 文 献

1) 社団法人音楽電子事業協会：MIDI 1.0 規格書，Rittor music.
2) The MIDI Manufactures Association: The Complete MIDI 1.0 Detailed Specification, document version 96.1 (1996).
3) 新井 純：SMF リファレンス・ブック，エディロール株式会社，東京 (1996).

4) 寺島情報企画：主なシーケンス・ソフトとその特徴，*DTM MAGAZINE*, Vol.112, p.41 (2003).
5) 井上大介，松本　勉：スタンダード MIDI ファイルステガノグラフィとその能力，情報処理学会論文誌，Vol.43, No.8, pp.2489–2501 (2002).
6) Inoue, D., Suzuki, M. and Matsumoto, T.: Detection-Resistant Steganography for Standard MIDI Files, *IEICE Trans.*, Vol.E86-A, No.8, pp.2099–2106 (2003).
7) 遠山　毅，鈴木雅貴，四方順司，松本　勉：編集ソフトウェアの特徴を利用する攻撃への耐性を有する演奏データファイル・ステガノグラフィの一方式，コンピュータセキュリティシンポジウム 2004 論文集，pp.85–90 (Oct. 2004).
8) 遠山　毅，鈴木雅貴，四方順司，松本　勉：編集ソフトウェアの特徴を利用する攻撃への耐性を有する SMF ステガノグラフィ方式の評価，2005 年暗号と情報セキュリティシンポジウム予稿集，pp.55–60 (Jan. 2005).
9) 岩切宗利，山本紘太郎，関根健一郎，松井甲子雄：電子演奏の半雑音化と音源符号への電子透かし，情報処理学会論文誌，Vol.43, No.2, pp.225–273 (2002).
10) 山本紘太郎，岩切宗利：発音の連接性を考慮した楽音符号への情報ハイディング，コンピュータセキュリティシンポジウム 2005 論文集，pp.565–570 (Oct. 2005).

(平成 18 年 11 月 27 日受付)
(平成 19 年 6 月 5 日採録)

遠山　毅

2004 年横浜国立大学工学部電子情報工学科卒業．2006 年同大学大学院環境情報学府情報メディア環境学専攻博士課程前期修了．現在，同大学院同専攻博士課程後期に在学中．情報ハイディングに興味を持つ．

鈴木　雅貴

2005 年 3 月横浜国立大学大学院環境情報学府博士課程後期修了．博士（工学）．同年 4 月より東京大学生産技術研究所に勤務．2006 年 4 月より日本銀行において情報セキュリティ技術の調査・研究に従事し，現在に至る．

四方　順司（正会員）

京都大学理学部数学科を卒業し，同大学大学院理学研究科数学・数理解析専攻修士課程を修了後，大阪大学大学院理学研究科数学専攻博士後期課程を修了し，博士（理学）を取得（2000 年 3 月）．2000 年 4 月から 2002 年 3 月まで東京大学生産技術研究所研究員として勤務．2002 年 4 月からは横浜国立大学大学院環境情報研究院に勤務．この間，講師，助教授を経て，現在は同大学大学院環境情報研究院准教授．専門分野は，暗号理論，情報セキュリティ，計算数論，計算機科学．これまでに，第 19 回電気通信普及財団賞・テレコムシステム技術賞（2004 年），電子情報通信学会 SCIS 20 周年記念賞（2003 年），同学会 SCIS 論文賞（2005 年）を受賞．

松本　勉（正会員）

情報セキュリティ，暗号，耐タンパ性，バイオメトリクス，人工物メトリクス，そのほか，情報学全般を専門とする．東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士（1986 年 3 月）．1986 年 4 月より横浜国立大学工学部に専任講師として勤務．同助教授，同教授を経て，2001 年 4 月より同大学大学院環境情報研究院教授．2007 年 4 月より社会環境と情報部門長を兼任．この間，日本銀行金融研究所客員研究員，カールスルーエ大学（ドイツ）客員教授，ケンブリッジ大学（イギリス）研究員，等を兼務．現在，国際暗号学会（IACR）理事．日本学術会議連携会員．CRYPTREC 暗号技術検討会構成員．暗号モジュール試験および認証制度（JCMVP）における技術審議委員会委員長．ISO/TC68（金融サービス）国内委員会委員長．電子情報通信学会平成 6 年度業績賞「情報セキュリティの基礎技術に関する先駆的研究」，2006 年，第 5 回ドコモ・モバイル・サイエンス賞・先端技術部門・優秀賞等を受賞．