

音声データにおける墨塗り署名ツール“SANI”の開発

石井 利晃

1. はじめに

近年、IC レコーダが普及し、会社での議事録作成や、大学での講義などで用いられる傾向がある。平成 14 年度以降は、文部科学省が推進しているサイバーキャンパス整備事業により、インターネットを介した学習支援システムの構築も進んでいる。東海大学も教育研究システム TICU(Tokai International Cyber University)を展開しているが、講義中の個人名などのプライバシー情報をそのまま公開するわけにはいかない。一方、デジタルコンテンツの偽造を防止するためにはデジタル署名が有効である。しかし、個人名やプライバシーに関する情報を削除してしまうと、署名の検証に失敗し、元のデジタルコンテンツと同一であることを保証できない。

そこで、本研究は、一部が削除されても署名の検証が可能な墨塗り署名ツールの開発を目的とする。対象は、IC レコーダなどの録音機器で使用されている音楽形式のひとつである WAV である。

2. 墨塗り署名

墨塗り署名は、署名者がある文書に対する署名を生成した後に、墨塗り者が文書の一部を変更(墨塗り)することを許容する署名方式である。[1]では電子文書への署名技術として提案されたが、本研究では音声データに対してこの署名技術を用いる。

2.1 SUMI-4

宮崎らによって提案されている墨塗り署名方式^[1]に、SUMI-4 がある。SUMI-4 では、オリジナルデータをN個のブロック $M_1, \dots, M_N$ に分割し、それぞれ乱数を $R_1, \dots, R_N$ を割り当て、それらのハッシュ値 $H_1, \dots, H_N$ の和に署名する。墨塗りを行う際には、データ M_i 、 R_i をハッシュ値 H_i に置き換える。ハッシュの一方方向性から、ハッシュの値から元のデータは判別不可能である。署名の生成と検証は、乱数 $R_1, \dots, R_N$ を結合したN個のデータのハッシュ値の結合に対して行う。

3. 提案方式

SUMI-4 はチャンクと呼ばれる単位からなっている WAV フォーマットに準拠して行う。

WAVの再生には、音声フォーマットを格納するfmtチャンクと波形データを格納するdataチャンクが必要である。これらは形式が定められており、他のデータを格納することができないため、乱数 $R_1, \dots, R_N$ をWAVに書き込むことがで

きない。そこで、音声の再生に影響しない余剰データを書き込むチャンク(randチャンク)を追加する。図 1 に、WAV 準拠の提案符号化方式を示す。



図 1. WAV 準拠の提案符号化方式

開発したツールは、署名ツールと墨塗りツール、検証ツールから成る。それぞれのツールでは、WAV ファイルの音声データと付加データに対して操作を行う。

4. 評価

データサイズのみが異なる音声ファイルに対する、署名生成、墨塗り、署名検証の時間を図 2 に示す。図 2 より、データサイズと署名生成、検証時間は入力データサイズに対して比例関係にあることがわかる。また、署名生成、検証に比べて、墨塗りには時間がかからない。

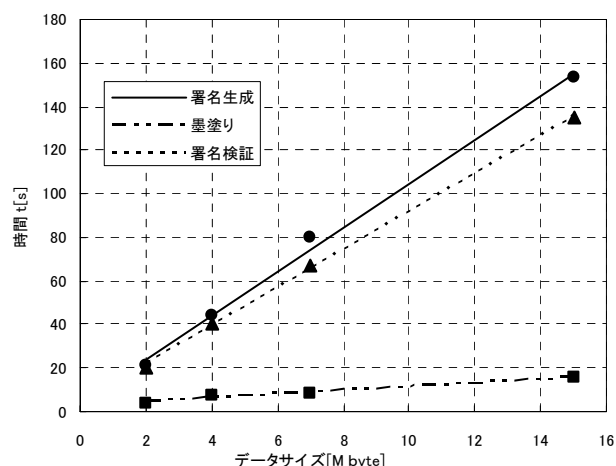


図 2. データサイズに対する署名生成、墨塗り、検証時間

5. おわりに

Java を用いて、音声データにおける墨塗り署名ツールを開発した。今後の課題として、動画ファイルへの応用や、WAV 以外にも署名を行えるようにする等が挙げられる。

参考文献

- [1] 宮崎 他: “電子文書墨塗り問題”, 電子文書通信学会 (ISEC2003), pp. 61-67, (2003).