OUKA
The University of Osaka
Institutional Knowledge Archive

Title	A Study on Low-Complexity Audio Encryption Methods for Digital Rights Management
Author(s)	Twe Ta Oo
Citation	大阪大学, 2015, 博士論文
Version Type	VoR
URL	https://doi.org/10.18910/53937
rights	Copyright(C)2014 IEICE
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

Form 3

Abstract of Thesis

Name (Twe Ta Oo)	
Title	A Study on Low-Complexity Audio Encryption Methods for Digital Rights Management (デジタル著作権保護のための音声信号の高速暗号化手法に関する研究)

Abstract of Thesis

This thesis discusses low-complexity audio encryption methods for Digital Rights Management (DRM). Recent years have seen the rapid growth of Internet traffic and the proliferated distribution of digitalized audio products such as music, audio books, and spoken news. As a result, secure distribution and copyright protection of those products have been increasingly important. The DRM technologies have been intensively studied in this area, and encryption plays an important role to protect the contents from unauthorized accesses. Although encryption ensures content security, the naive method of encrypting an audio file would destroy compliance with the audio standard so the resulting encrypted file could not be rendered by existing standard media players. This thesis focuses on low-complexity audio encryption methods that keep compliance with the media standard and achieve the following DRM requirements: 1) providing the confidentiality in audio distribution, 2) controllably degrading the audio quality by adjusting the percentage of encryption, and 3) realizing the try-before-purchase model, which is one of the important business models of DRM, in which the encrypted audio files are published for commercial purpose; users can render those files for trial without decryption and enjoy the contents in original quality by purchasing the decryption keys.

Firstly, this thesis presents a low-complexity partial encryption method for compressed audio (MP3). Unlike conventional encryption which encrypts the whole file, partial encryption can provide some interesting features such as yielding low-quality signals, reducing execution time, and coexistence with the media standards. The main idea of partial encryption is to protect the entire content by encrypting only the perceptually important parts. This thesis discusses how to choose the perceptually important parts during the MP3 encoding process in accordance with the concept of the Human Auditory System (HAS). Experimental results show that encrypting the whole MP3 file renders the audio signal meaningless while encrypting 2-10% of the file degrades the audio quality but not completely destroys the signal so it can be used as trial music. That trial MP3 keeps compatibility with the standard so it can be rendered by any existing MP3 players without need to decrypt. Under the access of the correct decryption keys and specific MP3 players, the full-quality MP3 can be successfully recovered. In addition, this thesis discusses the invalid amplitude problem regarding audio encryption: in any kinds of audio format, there are valid amplitude ranges for audio samples, which differ based on the supported bit-depth of an audio coder. If the audio samples to be coded are not within the valid range, they are clipped. This becomes a problem when the encrypted audio samples are beyond the valid ranges and get clipped because the data losses introduced by clipping deter the decryption process from successfully recovering the signal. This thesis also presents a solution for this problem.

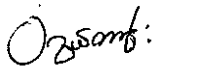
Secondly, this thesis presents two low-complexity audio scrambling methods, which are kinds but not direct applications of audio encryption. Unlike audio encryption that renders an audio signal meaningless by changing both the values and positions of the contents, audio scrambling degrades the residual intelligibility of an audio signal by breaking the coherence

between data contents. They neither inject any new values nor change the values of the existing contents. Due to this feature, they are more preferable to usual audio encryption to be used as pre- and post-processing of data hiding methods. This thesis presents two effective audio scrambling methods in the time domain: one based on the pre-order traversal of a complete binary tree and the other on a pseudorandom number generation algorithm called Mersenne Twister (MT). Experimental results show that the proposed methods are very effective in terms of time and space complexity and scrambling effect. However, their cryptographic security is limited because of the only use of permutation operations.

Thirdly, with the aim of strengthening the cryptographic security of the proposed audio scrambling methods, this thesis presents two new schemes in the wavelet domain. First, an audio signal is wavelet decomposed. Then, the layers of wavelet coefficients are separately scrambled by considering not only the pre-order but also in-/post-order based scrambling methods in the first scheme and using the MT based scrambling method with a series of keys in the second scheme. Experimental results show that anyone without knowledge of the correct wavelet decomposition parameters and the correct method/key used for each layer will not be able to successfully descramble the signal. The new schemes also achieve progressive scrambling that enables the audio outputs with different quality levels to be generated by controlling the scrambling degree on the basis of the system requirement: slightly distorted ones for the try-before-purchase model of the DRM systems and severely distorted ones for the systems with strong security needs.

As a conclusion, this thesis presents low-complexity audio encryption methods for both compressed and uncompressed audios with detailed discussions on 1) how to solve the invalid amplitude problem regarding audio encryption, 2) how to effectively choose the perceptually important parts for partial encryption, 3) how to conduct encryption while keeping compliance with the media format, and 4) how to strengthen the cryptographic security of audio scrambling. In addition to providing confidential audio distribution, the proposed methods can also be used to realize the try-before-purchase model. Thus, these proposals strongly contribute to the development of efficient DRM systems.

Name of Applicant: Twe Ta Oo



Name Stamp or Signature

様式 7

論文審査の結果の要旨及び担当者

氏　名　（　Twe Ta Oo　）		
	（職）	氏　名
論文審査担当者	主 査　教授	尾上 孝雄
	副 査　教授	土屋 達弘
	副 査　教授	申　吉浩（兵庫県立大学）
	副 査　准教授	橋本 昌宜

論文審査の結果の要旨

本論文は、デジタル著作権保護のための音声信号の高速暗号化に関する研究の成果をまとめたものであり、以下の主要な結果を得ている。

1. **圧縮符号化音声信号に対する部分暗号化手法の提案**

音声信号の暗号化は、信号全体に対して行われることが一般的であるが、本研究では、MP3 (MPEG Audio Layer-3) などの圧縮符号化された音声信号に対し、人間の聴覚特性を利用することで、聴覚認知に重要な信号のみを暗号化する手法を提案している。これにより、暗号化処理自体を高速に実行することを可能としている。加えて、従来は一旦暗号化すると全く音声信号が再生できなかったが、本手法を適用することにより、音質を低く抑えた音声信号を提供することが可能となっている。これは、音楽配信などにおけるトライアル視聴を容易に実現できるため有用である。

2. **音声信号に対するスクランブル手法の提案**

音声信号のセキュリティを担保するための方法としてスクランブル手法がある。前述の暗号化手法は単独では非常に有効に働くが、例えば著作権保護のために一般的に用いられている、電子透かしなどとの親和性は高くないとされている。これに対し、音声信号のスクランブル手法は、セキュリティを担保しつつ電子透かしなども容易に適用することが可能である。本論文では、2種類の音声信号スクランブル手法を提案している。二分木の前順走査に基づく方法とメルセンヌ・ツイスタ擬似乱数列生成器に基づく方法である。これらを音声信号に適用した実験結果から、両手法とも時間計算量、空間計算量ともに少なく高速に実行することが確認されている。一方で、置換処理のみに基づくため暗号化性能には改善の余地があることも指摘している。

3. **音声信号に対するウェーブレット領域スクランブル手法の提案**

上記で懸案となった、より強固なセキュリティの確保のため、本論文では、音声信号に対し、時間領域でなく周波数変換を行って周波数領域でスクランブルする手法を提案している。具体的には、ウェーブレット変換により分割された各周波数成分に対して、選択的にスクランブルを行う手法である。スクランブルには、前順走査、間順走査、後順走査のいずれかの方法、ならびにメルセンヌ・ツイスタ擬似乱数列生成器に基づく方法を提案している。本手法により、十分な暗号化性能を得られることが確認できるとともに、必要となるセキュリティレベルおよび音質に応じて階層的にスクランブルを行うことも可能としている。

以上のように、デジタル著作権保護のための音声信号の高速暗号化手法に関する研究は、今後ますます重要となるマルチメディア情報のネットワーク利用を促進するという側面からも非常に有用である。処理速度やセキュリティレベルに関しても議論されており、本論文はマルチメディア情報セキュリティの実用化にも寄与するものと期待できる。従って、博士（情報科学）の学位論文として価値あるものと認める。