A SPECIFICATION

FOR

A SYSTEM AND METHOD FOR LOSSLESS AUDIO ENCODING WITH INTEGRATED OFFLINE AUTHENTICATION AND DIGITAL RIGHTS MANAGEMENT

By Henry T. McBrien

10/12/2024

A system and method for lossless audio encoding is required in present market conditions. The system generates a digital audio file comprising a Main Audio Package (MAP) and an Authentication Key Message (AKM). The MAP contains losslessly compressed audio data, where compression is achieved through a combination of predictive coding and entropy encoding of residual signals. The AKM comprises cryptographic information for both file authentication and user-level access control. File authentication is performed offline using a digital signature created by hashing the MAP and encrypting the hash with a private key. User access is managed through Digital Rights Management (DRM) by encrypting a symmetric session key with a public key unique to an authorized user, where the session key is used to decrypt the MAP. This dual-layered security model provides robust file integrity verification and access control without requiring a continuous online connection.

SPECIFICATIONS

1 The field of digital audio has a need for secure, high-fidelity formats that ensure both the authenticity of the content and the control of its distribution. Existing formats often lack robust, integrated security features or require constant connectivity to a central server for

verification, which limits their utility in offline environments. There is a need for a unified system that can provide lossless audio quality while implementing cryptographic controls for file integrity and user access. The present invention addresses these deficiencies by providing a comprehensive, self-contained system for authenticated and encrypted lossless audio.

2 The present invention provides a method for generating a digital audio file format, hereinafter referred to as the "Dougsphere" format, which comprises two distinct but cryptographically linked components: a Main Audio Package (MAP) and an Authentication Key Message (AKM). The MAP contains the primary audio data, which is losslessly compressed to reduce file size while preserving audio fidelity. The AKM contains the necessary cryptographic data to perform offline authentication of the file's origin and to enforce Digital Rights Management (DRM) for user access.

2.1 The lossless compression of the MAP is achieved through a two-step process. First, an audio signal is processed by a predictive coding scheme, where each audio sample is predicted from preceding samples. The difference between the actual sample and the predicted sample, known as the residual, is then encoded. Second, these residuals are subjected to entropy encoding, such as Huffman or arithmetic coding, to efficiently represent the data.

2.2 The AKM facilitates a two-part security scheme. For file integrity and authenticity, a digital signature is generated by hashing the MAP and encrypting the hash with the content creator's private key. This signature is stored in the AKM. A receiving party can verify the file's authenticity by re-hashing the MAP and comparing it to the decrypted hash from the AKM. For user-level access and DRM, the MAP data is encrypted with a symmetric session key. This session key is, in turn, encrypted with a public key unique to an authorized user's license and stored within the AKM. A user can only decrypt and access the audio data if they possess the corresponding private key to unlock the session key.

2.3 The present invention supports multiple audio channels, such as up to 6 channels, and

includes Chain of Custody (CoC) controls within the AKM to trace the history of the file.

3 The MAP is a data container for the losslessly compressed audio. The compression methodology employs a Linear Predictive Coding (LPC) model. A predictor filter, defined by a set of coefficients, is applied to the audio signal. The residual signal, which represents the prediction error, is then calculated. The residual signal is statistically more compact than the original audio signal, as it tends to have a greater concentration of values around zero.

3.1 The residual signal is then processed by an entropy encoder. The encoder constructs a variable-length code table where frequently occurring residual values are assigned shorter bit sequences and less frequent values are assigned longer sequences. The resulting compressed bitstream is stored in the MAP.

3.2 The system used is interoperable with PCM encoding.

4 The AKM is a metadata container that resides alongside the MAP. It houses cryptographic and control information.

4.1 The AKM stores a digital signature. This signature is a cryptographic hash of the entire MAP data, signed with a private key owned by the content creator. Verification requires a user's software to re-calculate the hash of the MAP and compare it with the hash derived from the signature using the creator's public key.

4.2 The audio data within the MAP is encrypted using a strong symmetric algorithm, such as AES (Advanced Encryption Standard), with a unique session key. To enforce DRM, this session key is then encrypted using the public key from the authorized user's license. The encrypted session key is stored in the AKM. Playback software uses the user's private key to decrypt the session key, which then allows for the decryption and playback of the audio data.

4.3 The AKM may also contain additional metadata, such as a timestamp and a creator's identifier, to establish a chain of custody and verify the file's lineage.

CLAIM OF INVENTION

1 A method for generating a digital audio file, said method comprising:

1.1 receiving an uncompressed audio signal;

1.2 generating a Main Audio Package (MAP) by applying a lossless compression scheme to said audio signal, said scheme comprising:

1.2.1 predicting subsequent audio samples based on preceding samples;

1.2.2 calculating a residual signal from the difference between predicted and actual samples;

1.2.3 applying entropy encoding to said residual signal to generate compressed audio data;

1.3 generating an Authentication Key Message (AKM), wherein said AKM comprises:

1.3.1 a digital signature generated by hashing the MAP and encrypting said hash with a private key of a content creator; and

1.3.2 an encrypted symmetric session key for decrypting the MAP, wherein said session key is encrypted with a public key associated with a user's license.

2 The method of claim 1, wherein the prediction of subsequent audio samples is performed using a linear predictive coding (LPC) model.

3 The method of claim 1, wherein the entropy encoding is performed using Huffman coding or arithmetic coding.

4 The method of claim 1, wherein the digital audio file is configured for offline verification of authenticity and offline enforcement of user access rights.

5 A digital audio file format, comprising:

5.1 a Main Audio Package (MAP) containing losslessly compressed audio data; and

5.2 an Authentication Key Message (AKM) containing cryptographic information for said MAP, wherein said cryptographic information comprises:

5.2.1 a digital signature for authenticating the integrity and origin of the MAP; and

5.2.2 a symmetrically encrypted session key for decrypting the MAP, said session key being asymmetrically encrypted with a public key of an authorized user.

HENRY MCBRIEN

DESIGNER

THIS DOCUMENT

FOR RELEASE

DOUGTONE.COM

FOR FURTHER LICENSE QUESTIONS, CONTACT

WEBMASTER@DOUGTONE.COM