Abstract

A data processing apparatus a data processing method efficiently ascertain that data are valid, prevent encryption processing key data from leaking, eliminate illegal use of contents data, restrict contents utilization, apply a different plurality of data formats to contents and efficiently execute reproduction processing of compressed data. The verification process of partial data is executed by collating the integrity partial data as check values for a combination of partial data of a content, and the verification process of the entirety of the combination of partial data is executed by collating partial-integrity-check-value-verifying integrity check values that verify the combination of the partial integrity check values. Master keys to generate individual keys necessary for a process of such as data encryption are stored in the storage section and keys are generated as required. An illegal device list is stored in the header information of a content and referred to when data is used. Keys specific to a data processing apparatus and common keys are stored and the keys are selectively used according to the content use restriction. Plural content blocks are coupled, and at least a part of the content blocks is applied to an encryption process by an encryption key Kcon, then encryption key data that is the encryption key Kcon encrypted by an encryption key Kdis is stored in the header section. A content data is made of compression data and an expansion processing program or a combination of types of

compression programs and the reproducing apparatus can determine an expansion program applicable to a compressed content.