19 MAR 2003

ABSTRACT OF THE DISCLOSURE

A method and an apparatus allowing to ensure protecting digital data are provided.

In addition to re-encrypting the data by using an unchangeable key, the data is double re-encrypted by using a changeable key. The changeable key is used first and the unchangeable key is then used, or in another case, the unchangeable key is used first, and the changeable key is then used. In the aspect of embodiments, there is a case adopting a software, a case adopting a hardware, or a case adopting the software and the hardware in combination. The hardware using the unchangeable key developed for digital video is available. In adopting the software, encryption/decryption is performed in a region below the kernel where the user cannot handle to ensure the security for the program and for the key used. More concretely, encryption/decryption is performed in a filter driver, a device driver, i.e., a disk driver and a network driver, in an I/O manager and an RTOS using a HAL. Either one of two filter drivers, with a file system driver between them, may be used and further, both of them may be used.



162162

