

“iVDR-Secure” Solutions for Content-access Services

Yukihide Inagaki
Hirofumi Sukeda
Hiroo Okamoto
Tatsuya Hirai

OVERVIEW: The utilization of HDDs for reading/writing of large volumes of data at high speed has been spreading to applications such as TV program recording as well as audio and in-car equipment. Under this utilization scenario, to enable appealing content to be circulated, it is important to establish a content-protection system that ensures content to be provided securely without causing concern for violation of copyright. If a system is set up on a content-protection basis, however, content cannot be freely transferred, so the user ends up being inconvenienced. Hitachi is working on establishing “iVDR-Secure” solutions, which enable content regularly obtained by users for use on multiple devices in an integrated manner. iVDR-Secure is based on the concept of preventing illegal copying and use of content, thus protecting copyright revenues, while creating an environment that enables users to enjoy content without inconvenience anytime, anywhere. While pushing ahead with product development and support of iVDR-Secure-compatible devices, we will continue to offer new “content-access services.”

INTRODUCTION

WITH the popularization of broadband access and digital broadcasting and the digitization of information, the applications of HDDs (hard disk drives)—which can read and write large amounts of data at high speed—continue to expand into fields such as TV-program recording as well as audio and in-car devices.

Since recording density of HDDs has been improved in increments shorter than the lifetime of AV (audio-visual) equipment, the recording capacity of devices fitted with permanent HDDs soon becomes obsolete; thus, users cannot adequately share in the benefits from improved HDD capacity. Moreover, the increase in capacity of compact HDDs of 2.5 inches

and below is continuing, and as “removable” compact HDDs, such HDDs have thus made it possible to improve the convenience for users in handling a cross-section of various devices. Under these circumstances, iVDR (information versatile disk for removable usage)⁽¹⁾ has appeared as the standard for such removable HDDs. As a member of this standardization body, Hitachi is actively engaged in promoting iVDR (see Fig. 1).

To fully utilize the advantages of iVDR and expands its applications, it is important to set up a content-protection system so that appealing content can be provided securely without having to worry about playback or recording in violation of copyright.

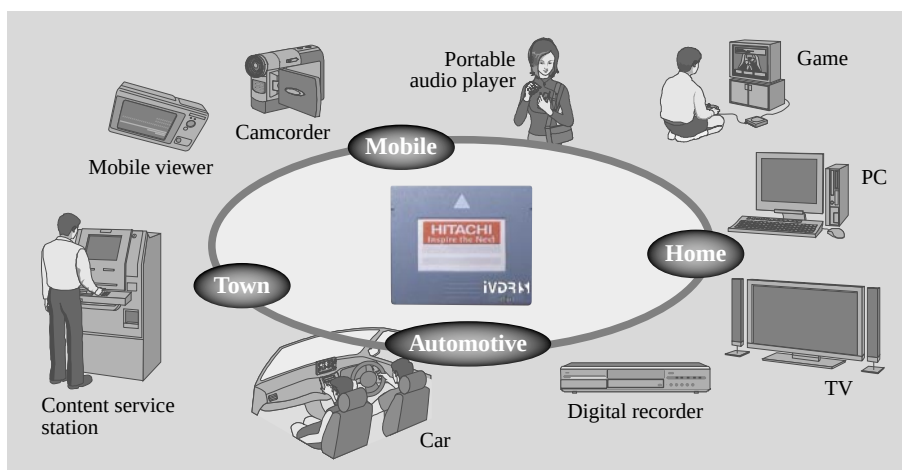


Fig. 1—The Diverse World Covered by iVDR-Secure.

Aimed at the “intelligent media” iVDR (information versatile disk for removable usage) for handling a wide range of applications from digital home appliances to PCs, an impregnable content-secure environment with mutual authentication is provided. By means of iVDR (called “iVDR-Secure”), applications starting with “digital-broadcast recording” and covering “audio” and “distribution” are sequentially dealt with.

In the rest of this paper, a content-protection system for removable HDDs—namely, iVDR—and some "iVDR solutions" are described.

NEEDS AND CHALLENGES CONCERNING REMOVABLE MEDIA

Compared with digital recording media, the performance of HDDs in terms of recording capacity and access speed is superior. On top of that, HDDs have the special characteristic that their recording capacity can be increased without affecting hardware compatibility. Traditional AV equipment has been used with an HDD in a permanently installed form. With the rapid advances in recording density of HDDs, however, a situation in which it is difficult for users to fully enjoy their AV equipment up to the timing of its replacement has arisen. Moreover, upgrading capacity and exchange/pick-up at the factory are extremely inconvenient compared with separated-type recording media. Furthermore, even with transfer of HDDs between rooms being impossible, straddling use in multiple devices and transfer of contents amassed up to replacement of AV equipment have been inhibited.

To address the above-described challenges, iVDR—being standardized in terms of form factors, interfaces, etc. as well as making HDDs removable—is being put forward. iVDR is aimed at creating compatibility between AV equipment, PCs, etc. and enabling integrated usage across such devices.

As regards conventional AV equipment with internal fixed HDDs, to prevent illegal copying and use of content, content is protected by methods such as applying a unique encryption to each device in correspondence with specific content on its HDD. In the case of such encryption methods, the content itself is "bound" to each device, so even if it is temporarily copied on another device, it cannot be used. In the case of recording media like removable iVDR, if the same content-protection method is used, while removable usage is possible, it cannot be used across a cross-section of devices. As a consequence, adequately exploiting the special features of removable media involves major challenges, namely, introducing a content-protection method bound with the media and preventing illegal copying while constructing a specification enabling an iVDR and its transferred content to be used on other devices.

COPYRIGHT-PROTECTION TECHNOLOGY iVDR Hard Disk Drive

The removable disk cartridge of iVDR comes in

three sizes, 1.0-inch, 1.8-inch, and 2.5-inch, covering low-capacity mobile use up to high-capacity home use (see Fig. 2). Equipped with content-protection technology called "Security Architecture for Intelligent Attachment Device (SAFIA)," these iVDRs are designated as "iVDR-Secure." Developed under the SAFIA License Group ⁽²⁾ (composed of Hitachi, Ltd., PIONEER CORPORATION, SANYO Electric Co., Ltd., and Sharp Corporation), SAFIA was licensed in November 2005.

As regards built-in 3.5-inch HDDs, SAFIA content-protection technology installed in normal HDDs is specified as "built-in-type iVDR-Secure" that does not require a special cartridge. It is being assumed that iVDR-Secure will be adopted by devices that require a large recording capacity, such as HDTV (high-definition TV) recorders.

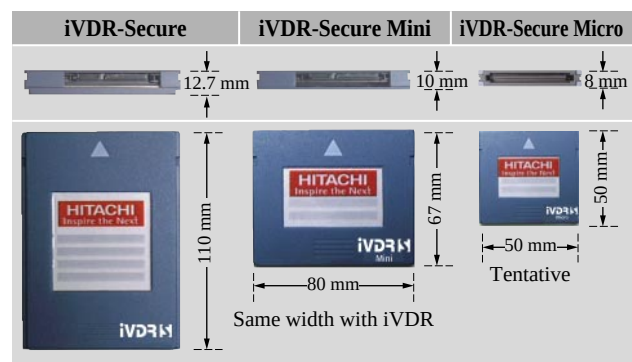


Fig. 2—The iVDR Family.
From left: 2.5-inch (iVDR), 1.8-inch (iVDR mini), 1.0-inch [iVDR micro (interim spec.)]

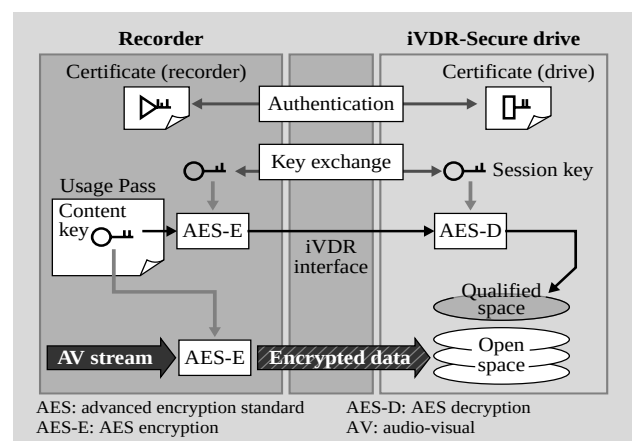


Fig. 3—Technical Outline of iVDR-Secure.
Both devices authenticate the other party, and an arrangement in which a "Usage Pass" (combining a content key and usage conditions) is encrypted and transferred is set up. AV streaming data is encrypted with a content key within the content path, and stored on "open space" on the iVDR drive.

TABLE 1. Specification Structure of iVDR and SAFIA
Covering audio specifications, etc.,
standardization plans are set out
consecutively.

Layer	Specification	iVDR specifications	SAFIA specifications
Rule			Compliance, robustness rules
Data format for application		TV recording	TV recording
		Audio recording	Storage device
		Picture recording	Other device (future)
		Others	Protocol and data structure
File system		iVDR file system	File system for iVDR
Interface		iVDR interface	Interface for iVDR
Physical/electrical		Hardware	

SAFIA: security architecture for intelligent attachment device

Basic Technology and Principle

SAFIA used in iVDR-Secure is a content-protection technology with the following special features (see Fig. 3).

- (1) Content encryption by AES (advanced encryption standard)-128 and impregnable security by transfer protocol and two-way authentication based on PKI (public key infrastructure)
- (2) Secure content access by means of a method that handles a content-encryption key and contents-utilization condition as a unit
- (3) Features of HDDs are made use of, assuring high-speed and secure contents movements.
- (4) Handling of “superdistribution⁽³⁾” for distributing routes (on which content data and keys are independent) at a certain timing

The structure of the technical specifications stipulating each respective SAFIA and iVDR is given in Table 1.

Presently, as an application layer of SAFIA, storage suitable for iVDR and TV recording/playback specifications are prescribed. From now onwards, it is planned to start specification designation for new applications according to need.

EXAMPLE APPLICATION OF iVDR-SECURE

Considering the user benefit from various viewpoints, Hitachi is establishing content-protection solutions that utilize iVDR-Secure. An example of such a solution is described in the following.

Digital-broadcast Recording

The foremost target of iVDR-Secure was application to digital-broadcast recording. As regards permanent HDDs installed in conventional digital TVs, content protection is set up so that the end user cannot change the combination of the HDD and the main device body. Accordingly, replacing the HDD on

failure or upgrading it is not easy. In contrast, iVDR-Secure enables mutual authentication between the HDD and the main body to be performed automatically and securely immediately after the HDD is changed, allowing the end user to easily exchange HDDs.

The benefit of being able to extend HDD into the hands of end users is huge. When a device is purchased, people are not so bothered with the capacity of the built-in HDD, and a buying pattern in which new iVDR-Secure devices are bought freely when users are confronted with a lack of storage space is being assumed.

Moreover, in March 2006, recognition of iVDR-Secure for digital-broadcast recording in Japan was received from The Association for Promotion of Digital Broadcasting (D-pa) and from The Association for Promotion of Satellite Broadcasting (BPA).

“My iVDR”

With the increase in capacity of recording media, the problem of how to organize large amounts of data has arisen. It can be assumed that in the case of multiple users, data can be accidentally accessed by other users, and out of consideration for other users, recorded data cannot be arranged freely as desired. However, if iVDR is used, everyone has their own iVDR (i.e. “My iVDR”), so one’s favorite music and often-used information can be carried around and kept apart from the likes and interests of others. Alternatively, a single user could possess multiple iVDRs, thereby expanding the way of using iVDRs—namely, by separately using iVDRs according to grouped content or intended applications and locations.

“Bridge” Media

In the case of replacement purchase of devices equipped with permanent large-capacity HDDs, it is possible that all the data accumulated up till then be

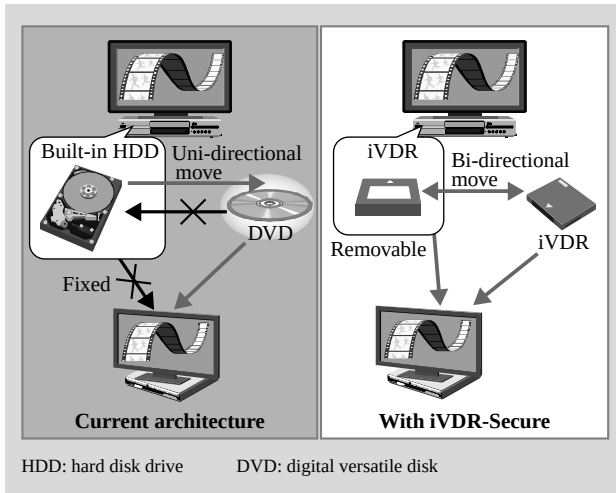


Fig. 4—Improved Freedom of Digital-broadcast Recording. When extracting recorded content and securing vacant HDD capacity, transfer to optical disk is not required.

lost. If iVDR is used, however, one's own content can be withdrawn from the old device at the time of disposal and used as is on the newly purchased device. Moreover, with the spread of iVDR-Secure-compatible devices, iVDR-Secure will act as a "bridge," making it possible to carry about content in an integrated manner between various household AV equipment and PCs.

In regard to recording of digital TV programs, owing to the "copy once" and the "content transfer" restrictions between built-in HDDs and DVDs, it is possible that inconvenience be imposed on users, even when content is transferred or cleared out. By handling two-way content transfer on removable media, iVDR-

Secure is expected to greatly improve user convenience (see Fig. 4).

Content-access Services

iVDR-Secure is a technology for handling so-called "superdistribution" (namely, enabling setup and distribution of content and keys independently), and its application to new "content-access services" like music, video, and maps is under investigation.

CONCLUSIONS

In this article, iVDR-Secure—a kind of removable HDD equipped with content-protection capability—was described. Content-protection technology provides a framework for providing content with peace of mind in regard to content copyrights. By applying iVDR-Secure, the content business is expected to be expanded and, at the same time, the ease of use for users, focused on access to content, can be improved. Taking account of the needs of users and current challenges, Hitachi is pushing ahead with providing services and new products that utilize removable, large-capacity media.

REFERENCES

- (1) iVDR Hard Disk Drive Consortium (iVDR Consortium), <http://www.ivdr.org/>
- (2) Security Architecture for Intelligent Attachment Device (SAFIA), <http://www.safia-lb.com/>
- (3) R. Mori et al., "Superdistribution as a Historical Inevitability," Information Processing Society of Japan, Architecture Symposium on "Supercompilation, Superdistribution, and Supermanagement," collected papers, Vol. 94, No. 1, pp. 67-76 (1994) in Japanese.

ABOUT THE AUTHORS



Yukihide Inagaki
Joined Hitachi, Ltd. in 1991, and now works at the HDD Architecture Research Unit of the Storage Technology Research Center, the Central Research Laboratory. He is currently engaged in the research of information/content protection system.



Hirofumi Sukeda
Joined Hitachi, Ltd. in 1985, and now works at the Contents Access Business Center, the Ubiquitous Security Division, the Security Systems Division, the Information & Telecommunication Systems. He is currently engaged in the business on contents access. Mr. Sukeda is a member of The Japan Society of Applied Physics (JSAP), Information Technology Standards Commission of Japan (ITSCJ).



Hiroo Okamoto
Joined Hitachi, Ltd. in 1980, and now works at the Storage Systems Research Center of the Ubiquitous Platform Systems R&D Laboratory, the Ubiquitous Platform Systems. He is currently engaged in the development of content protection technologies. Mr. Okamoto is a member of The Institute of Electronics, Information and Communication Engineers (IEICE).



Tatsuya Hirai
Joined Hitachi, Ltd. in 1994, and now works at the HDD Architecture Unit of the Magnetic Drive Technology Research Department, the Storage Technology Research Center, the Central Research Laboratory. He is currently engaged in the Standardization of SAFIA technology and technical support for developing iVDR drive and appliances with SAFIA functions. Mr. Hirai is a member of IEICE.