

Method of Protecting Recorded Multimedia Content Against Unauthorized Duplication

ABSTRACT

Protection against unauthorized access to stored content on a video appliance such as a set-top box/PVR (Personal Video Recorder) is provided by encrypting stored content using an event key derived by hashing a base key unique to the set-top box/PVR with event-specific information unique to the stored content. A content handle derived from the event-specific information (and optionally identical thereto) is stored along with the encrypted stored content, identifying it. To decrypt an item of stored content, the event key is recreated by once again hashing the base key (securely stored within the set-top box) with the event-specific information associated with the item of stored content (re-derived from the content handle, as necessary). This event key, identical to the event key used to encrypt the stored content, is then used to decrypt it, making it available for playback. Unauthorized access to deleted content is prevented by erasing (e.g., overwriting) the content handle associated with the deleted content.

Fig. 1