TECHNOLOGY

Method and Apparatus for Conditional Access in Broadcast/Multicast Systems

OVERVIEW

Following the rapid expansion of the commercial broadcasting industry, conditional access systems have been deployed extensively to meet consumers' needs. These systems are used to provide services to authorized customers such as cable TV subscribers. In fact, some programs are only accessible to those who have made payments to the program providers. In today's growing E-commerce environment, conditional access is imperative to profitable digital broadcasting.

Current digital video broadcasting systems use a scrambler to implement encryption. Typically, the bit stream of a MPEG-2 encoder/multiplexer is fed into the scrambler unit along with the scrambler key. This key is encrypted and then sent to the receiver. A conditional access unit in the receiver will decrypt the key. However, this traditional approach involves complex computations on an ASIC due to the high date rate requirement, which also adds costs to the providers and their customers.

Researchers at the University of Maryland have developed a low-cost and reliable conditional access scheme to combat the above-mentioned problem. The novel approach successfully utilizes arithmetic coding to achieve encryption purposes for conditional access in digital broadcast systems at a lower cost. Further, an adaptive source symbol frequency model is used, which adds more security to the system. For example, an unauthorized user who tries to attack such a conditional access system will not be able to determine the proper position of the sequence of the bits, or the number of symbols in the adaptive frequency model. Both parameters are critical to successful cryptanalysis.

Taking advantage of the cryptographic properties of the arithmetic coding, the researchers have demonstrated that the new scheme is capable of considerably decreasing the amount of data that needs to be processed for scrambling. In comparison with the current conditional access systems, the UM scheme has the following advantageous features:

1.The computational load of the encryption unit is reduced because the new scheme requires a smaller amount of information in the frame headers for encryption.
2.The increased computational simplicity and flexibility allow for a low cost processor to complete the encryption tasks.
3.The new scheme can be implemented on existing conditional access systems with no additional cost of extra hardware.

For licensing information, please contact the Office of Technology Commercialization at the University of Maryland, phone (301)405-3947 or e-mail: otc@umd.edu

CONTACT INFO

UM Ventures
0134 Lee Building
7809 Regents Drive
College Park, MD 20742
Email: umdtechtransfer@umd.edu
Phone: (301) 405-3947 | Fax: (301) 314-9502

Additional Information

INSTITUTION

University of Maryland, College Park

PATENT STATUS

U.S. Patent # 7,006,568

LICENSE STATUS

Available for exclusive license

CATEGORIES

- Microelectronics
- Information Technology

EXTERNAL RESOURCES

- US Patent 7,006,568

IS-99-028