ABSTRACT OF THE DISCLOSURE

PAY BROADCASTING SYSTEM WITH ENHANCED SECURITY AGAINST ILLEGAL ACCESS TO A DOWN LOADED PROGRAM IN A SUBSCRIBER TERMINAL

In a pay broadcasting system, data of a broadcast program is scrambled with a scramble key updated in a short period. The scramble key is encrypted with a first key assigned to the subscriber terminal. The first key is encrypted with a first master key set in the subscriber terminal. The security of a broadcast program stored for subsequent use in the subscriber terminal is enhanced as follows. A central station generates a second key-encrypted scramble key by encrypting the scramble key with a second key different from the first key and changeable in an interval shorter than a update interval of the first key; generates an encrypted second key by encrypting the second key with a second master key which has been commonly issued to subscriber terminals of the system; and broadcast the second key-encrypted scramble key and the encrypted second key together with the scrambled data of the program, the first key-encrypted scramble key and the encrypted first key in a multiplexed manner. When a broadcast program is to be stored, the subscriber terminal stores the scrambled data of the broadcast program and the second key-encrypted scramble key; decrypt the encrypted second key with the second master key into the second key, which is added to a stored program second key list. If the stored program is to be executed, the second key-encrypted scramble key is decrypted with a corresponding one of the second keys in the stored program second key list into a decrypted scramble key; and the scrambled data of the broadcast program is unscrambled with the decrypted scramble key.

Figure 4.